Security Intelligence of Broadcast: Threat Analytics

Sumit Chakraborty
Fellow, Management Information Systems (Indian Institute of Management Calcutta), BEE (Jadavpur University), India
E-mail: surya20046@yahoo.co.in, schakraborty2010@hotmail.com; Phone: 91-9940433441

Abstract: This work presents an Adaptively Secure Broadcast Mechanism (ASBM) based on threats analytics. It defines the security intelligence of a broadcast system comprehensively with a novel concept of collective intelligence. The algorithmic mechanism is analyzed from the perspectives of security intelligence, communication complexity and computational intelligence. The security intelligence of ASBM is defined in terms of authentication, authorization, correct identification, privacy: group, forward and backward, confidentiality and audit; fairness, correctness, transparency, accountability, trust, non-repudiation and data integrity; reliability, consistency, liveness, deadlock-freeness, safety and reachability. The computational intelligence is associated with the complexity of broadcast scheduling, verification of security intelligence of broadcasting system, key management strategies and payment function computation. The cost of communication depends on number of agents and subgroups in the broadcasting group and complexity of data. The business intelligence depends on payment function and quality of data stream. ASBM recommends a set of intelligent model checking moves for the verification of security intelligence of the broadcasting system. The primary objective of ASBM is to improve the quality of broadcast through fundamental rethinking and radical redesign of a reliable communication schema. This work also outlines the architecture of an automated system verification tool for the protection of the broadcasting system.
In the existing works of adaptively secure broadcast, broadcast corruption is not assessed properly. The issues of broadcast corruption have been defined imprecisely and incompletely through statistical reasoning. A broadcast protocol allows a sender to distribute a secret through a point-to-point network to a set of recipients such that (i) all recipients get the same data even if the sender is corrupted and (ii) it is the sender's data if it is honest. Broadcast protocols satisfying these properties are known to exist if and only if $t < n/3$, where n denotes the total number of parties, and t denotes the maximal number of corruptions. When a setup allowing signatures is available to the parties, then such protocols exist even for $t < n$. In the current work, the flaws of aforesaid bounds are corrected through case based reasoning of miscellaneous broadcast applications technically through a set of test cases. It is not rational to state the bound of adaptively secure broadcast protocol in a simple straight forward way. *Adaptively secure broadcast mechanism (ASBM) results correct and fair output if and only if all the agents (sending agent, receiving agents and broadcast system administrator), communication channel, broadcast mechanism, broadcast data, payment function and payment mechanism are free of corruption.* Here, the risks of broadcast corruption are assessed and mitigated through collective security intelligence on ASBM. First, this works designs ASBM which is more complex than the existing adaptively secure broadcast protocol and then explores the corruption of ASBM from different angles. The concept of collective security intelligence is important to design robust, stable and secure auction, reverse auction, combinatorial auction and multi-party negotiation protocols in various types of broadcast applications. An isolated approach or focus on a specific type of threats cannot solve the ultimate problem of adaptively secure broadcast. The algorithm is applicable to the analysis of intelligent mechanisms in static and dynamic networks, auction or combinatorial auction for e-market, digital content distribution through computational advertising, cloud computing, radio and digital TV broadcast, SCADA and sensor networks.
Keywords: Broadcast Mechanism, Security intelligence, Computational intelligence, Communication complexity, Threat analytics, Automated system verification.

1. INTRODUCTION

Broadcast is one of the most fundamental concepts in distributed cryptography. It is an efficient mechanism for scalable information distribution where P2P communication faces the problem of

scalability. A central entity wishes to broadcast a secret data stream to a dynamically changing privileged subset of the recipients in such a way that non-members of the privileged class cannot learn the secret. Here, the critical objective is to optimize the cost of communication, the computation effort involved in key construction and the number of keys associated with each recipient. A broadcasting system is vulnerable to various types of malicious attacks. An adaptively secure broadcasting system is expected to be a *resilient system*. The resiliency measures the ability to and the speed at which the system can return to normal performance level following a disruption. The vulnerability of a broadcasting system to a disruptive event or threat should be viewed as a combination of likelihood of a disruption and its potential severity. It is essential to do two critical tasks: assess risks and mitigate the assessed risks. To assess risks, the security intelligence of the broadcasting system should be explored: what can go wrong in a broadcasting mechanism? what is the probability of the disruption? how severe it will be? what are the consequences if the disruption occurs? One of the top ten technology trends today is the design of advanced information security system. Adaptively secure broadcast falls in this category.

The security issues of a broadcasting system have been extensively studied in [1,2,3,4,5,6,7,8,9,10,11,32]. This work has reviewed TESLA and BiBa authentication protocols for secure multicast [2,3]. TESLA is a broadcast authentication protocol where the sender is loosely time synchronized with the recipients BiBa broadcast authentication protocol is based on BiBa (bins and balls) signature. It provides instant authentication; neither the sender nor the receivers buffer any data. It has a higher computation and communication overhead than TESLA. These broadcast authentication protocols require time synchronization. It is really challenging to develop a secure, efficient, real-time and scalable authentication mechanism with small digital signature size which does not require any time synchronization. The review of existing literature could not find out an efficient broadcast mechanism from the perspectives of security intelligence, business intelligence, computational and communication complexity. The existing works have several gaps. The security intelligence of a broadcasting system has been defined weakly, incompletely and imprecisely. The broadcast protocols lack intelligent model checking or system verification mechanisms based on rational threat analytics.

The contributions of the present work are as follows. This work presents an adaptively secure broadcast mechanism (ASBM) based on threats analytics and case based reasoning. It defines the security intelligence of an adaptively secure broadcast mechanism comprehensively. It explores the risk of different types of new attacks on the broadcasting system. The algorithmic mechanism is designed in terms of agents, input, output, network topology, communication model, broadcast mechanism and revelation principle. It recommends a set of intelligent model checking moves for the verification of security intelligence of the broadcasting mechanism. The mechanism is analyzed from the perspectives of communication complexity, computational intelligence, security intelligence, business intelligence, reliability, scalability and traffic congestion. The research methodology adopted in the present work includes case based reasoning, threat analytics and review of relevant literature on broadcast. The logic of the ASBM is explored through case based reasoning on e-market, wired and wireless communication network, internet, sensor network, mobile adhoc network, defense, SCADA, air traffic control system, logistics and fleet monitoring system and flocking. The security intelligence is explored through threats analytics. The model checking algorithm assesses the risks of various malicious attacks and the relevant risk mitigation plans. The basic building blocks of the proposed algorithmic mechanism are information and network security, distributed cryptography and algorithmic game theory [12].

The work is organized as follows. Section 1 starts with introduction which defines the problem of adaptively secure broadcast. It reviews existing literature and analyzes the gaps, states research methodology and contributions of the work. Section 2 presents adaptively secure broadcast mechanism (ASBM). Section 3 analyzes ASBM in terms of security intelligence, computational and communication complexity. Section 4 outlines the system architecture and section 5 concludes the work.

2. ADAPTIVELY SECURE BROADCAST MECHANISM (ASBM)

Assumptions: (a) Broadcast communication must satisfy the basic requirements of security and privacy from the perspectives of collective intelligence of a rich knowledge base. (b) The analytics must explore the risk of all possible threats on a broadcasting system. (c) Another critical issue is low computation and

communication overhead for security intelligence. (d) The broadcasting system must support scalability and reliability. The sender tries to distribute real-time data reliably through a private communication channel, the recipients validate and use the received data as it arrives. Reliability detects missing or corrupted data.

Notations used in ASBM : S **-** Sending agent, R - Receiving agent, A - System administrator or regulator, C - Case, M - Move, T - Threat, V - Verification, P_d - Demand plan [d, b] where d is demand and b is the budget of a receiving agent, $D_{j;\ j=1,..,x}$ - Data stream in digital or analog signal (e.g. direction, speed, vision) to be broadcasted by the sending agent to the receiving agents, 1-n : one-to-many communication, m-n:many-to-many communication, p - combinatorial factors, P_b - Broadcast plan, p_f - payment function, t_r - maximum response time, n' - number of requests meeting the deadline, T - sum of response time, r - revenue; t_d : time deadline, m' - profit margin of S, FIFO - First-In-First-Out, LIFO - Last-In-First-Out, SI - security intelligence of the broadcasting system, QoS - Quality of Service, k_e - encryption key, k_d - decryption key.

Adaptively Secure Broadcast Mechanism (ASBM):

Agents: {S, $R_{i;i=1,..,n}$, A}; *or* {S, $R_{i;i=1,..,n}$};
Network Topology: Dynamic *or* Static network;
Communication model: 1-n *or* m-n *or* 1-n-p *or* m-n-p;
Input: Data stream $D_{j;\ j=1,..,x}$ *or* secret (D);
Broadcast Mechanism:

1. $R \rightarrow S : P_d$ [d, b];
2. $R \leftrightarrow S : [P_b, p_f]$;
   objectives: {minimize t_r, minimize n', minimize T, maximize r} subject to
   constraints: { time deadline : $t \leq t_d$, budget : $b \leq b_{max}$, profit margin : $m_{min} \leq m' \leq m_{max}$ };
   moves : select single or multiple moves from { FIFO, LIFO, priority queue, load consolidation, data filtering, unidirectional communication, bidirectional communication, synchronous communication, asynchronous communication, single round communication, multiple rounds communication};
   payment function: *commit* on (P_b, p_f) through multi-party negotiation *or* swing option;

3. **Broadcast authentication protocol**:

3.1 *Sender's set up* : S generates, refreshes adaptively and distributes keys to R for private broadcast : (encryption and decryption) *or* digital signature *or* (signcryption and unsigncryption) *or* privacy preserving data mining (ppdm : randomization, summarization, aggregation, generalization, suppression, de-identification and k-anonymity);

3.2 *Receiver's set up* : The recipients acknowledge S after the receipt of authentication keys.

3.3 $S \rightarrow R_{i;i=1,..,n}$: broadcasts encrypted data $D' = \{ D_{;j=1,..k}\}_{ke}$ *or* non-encrypted data D *or* perception of signal by R from S without using any channel;

3.4. $R_{i;i=1,..,n}$: decrypts or unsigncrypts data. $\{D'\}_{kd}$, or receives D.

4. Verify **security intelligence** through automated or semi-automated system verification**.**

4.1 call *threat analytics* and assess risks of single or multiple attacks on broadcasting system; analyze performance, sensitivity, trends, exception and alerts.

4.1.1 what is corrupted or compromised: agents, communication schema, data schema, application schema, computing schema and broadcast mechanism?

4.1.2 time : what occurred? what is occuring? what will occur? assess probability of occurrence and impact.

4.1.3 insights : how and why did it occur? do cause-effect analysis.

4.1.4 recommend : what is the next best action?

4.1.5 predict : what is the best or worst that can happen?

4.2 do verification of security intelligence in terms of authentication, authorization, correct identification, privacy: group, forward and backward, audit; fairness, correctness, transparency, accountability, confidentiality, trust, integrity, non-repudiation, commitment, reliability, consistency; liveness, deadlock freeness, lack of synchronization, safety and reachability;

4.3 Assess and mitigate the risks of false data injection, sybil, node replication, wormhole, blackhole, jellyfish, rushing, neighbor, coremelt, node deletion, flaws in broadcast schedule, poor QoS,

malicious business intelligence, corruption in secret sharing, information leakage, replay and shilling attack *[Refer section 3.1 : Model Checking Algorithm]*.

5. The honest agents compute penalty function and charge the corrupted agents; mitigate risk of threats through regulatory compliance.

Output: Broadcast plan (P_b), Security intelligence of broadcasting system.

3. COMPLEXITY ANALYSIS of ASBM

This section analyzes the complexity of adaptively secure broadcast mechanism in terms of communication complexity, computational intelligence, security intelligence and business intelligence. The complexity analysis is important to define the system architecture of a broadcasting system in terms of application, computing, data, networking and security schema. The mechanism is analyzed in terms of agents, network topology, communication model and broadcast mechanism. The agents negotiate broadcast plan based on objectives, constraints, strategic moves and payment function. The broadcast mechanism has two critical parts: broadcast authentication protocol and verification of security intelligence. The risks of various types of malicious attacks are assessed and mitigated by calling model checking algorithm. The algorithm is presented in section 3.1.

3.1 Security Intelligence

Theorem 1: The security intelligence of ASBM is defined comprehensively through a set of properties of secure multi-party computation based on collective intelligence. It is explored through rational threat analytics.

The security intelligence of ASBM is defined with a novel concept of collective intelligence and in terms of a set of properties of secure multi-party computation: authentication, authorization, correct identification, privacy: group, forward and backward, confidentiality and audit; fairness, correctness, transparency, accountability, trust, non-repudiation and data integrity; reliability, consistency, liveness, deadlock-freeness, safety and reachability. ASBM must address correct identification, authentication, authorization, privacy and audit for each broadcast session. For any secure service, the system should ask the identity and authentication of one or more agents involved in a communication. The agents of the same trust zone may skip authentication but it is essential for all sensitive communication across different trust boundaries. After the identification and authentication, a service should address the issue of authorization. The system should be configured in such a way that an unauthorized agent cannot perform any task out of scope. The system should ask the credentials of the requester; validate the credentials and authorize the agents to perform a specific task as per agreed protocol. Each agent should be assigned an explicit set of access rights according to role. Privacy is another important issue; an agent can view only the information according to authorized access rights. A protocol preserves privacy if no agent learns anything more than its output; the only information that should be disclosed about other agent's inputs is what can be derived from the output itself. The privacy of data may be preserved in different ways such as adding random noise to data, splitting a message into multiple parts randomly and sending each part to an agent through a number of parties hiding the identity of the source, controlling the sequence of passing selected messages from an agent to others through serial or parallel mode of communication, dynamically modifying the sequence of events and agents through random selection and permuting the sequence of messages randomly. The agents must commit the confidentiality of broadcasted data in case of private communication of sensitive applications (e.g. defense, auction). The system administrator must be able to audit the efficiency of broadcasting mechanism at anytime in terms of fairness, correctness, transparency, accountability, confidentiality and trust.

There are some other important parameters of security intelligence: fairness, correctness, transparency, accountability and trust. A broadcast protocol ensures correctness if the sending agent broadcasts correct data free from any false data injection attack and each recipient receives the same correct data in time without any change and modification done by any malicious agent. The fairness of the broadcast mechanism is associated with the commitment, honesty and rational reasoning on payment function, trust and quality of service. Fairness ensures that something will or will not occur infinitely often under certain conditions. The recipients expect fairness in broadcast communication according to their demands plan, objectives and constraints. The broadcaster expects fairness from the recipients in terms of true

feedback and commitment on confidentiality of broadcast data. The mechanism must ensure the accountability and responsibility of the agents in access control, data integrity and non-repudiation. The transparency of the broadcast mechanism is associated with communication protocols, revelation principle and automated system verification procedures. In fact, the issues of correctness, fairness, transparency and accountability are all interlinked.

There are some other important parameters of security intelligence for a broadcasting system. The performance of the broadcasting data stream and quality of service is expected to be consistent and reliable. Reachability ensures that some particular state or situation can be reached. Safety indicates that under certain conditions, an event never occurs. Liveness ensures that under certain conditions an event will ultimately occur. Deadlock freeness indicates that a system can never be in a state in which no progress is possible; this indicates the correctness of a real-time dynamic system.

The broadcasting mechanism calls threat analytics: assesses risks of single or multiple threats on the broadcasting system such as false data injection attack, sybil, node replication, wormhole, blackhole, jellyfish, rushing, neighbor, coremelt, node deletion, flaws in broadcast schedule, poor QoS, malicious business intelligence, shilling, corruption in secret sharing and information leakage through weak security algorithms [22,23].

A malicious agent can exploit the configuration of a broadcasting system to launch false data injection attack against state estimation and introduce arbitrary errors into certain state variables. It is very common in today's broadcast from digital media (e.g. news, budget, voting results, got up game etc.). In an open environment, sensor nodes operate without any supervision; a malicious attacker can capture a node for reconfiguration or extract the private data stored in the node through cryptanalysis. An attacker may be able to deploy multiple physical nodes with same identity through cloning or node replication attack. An adversary may be able to deploy multiple identities of a node to affect the trust and reputation of a broadcasting system through Sybil attack. The attacker may be able to build an additional communication channel to capture private communication in sensor network through wormhole attack.

A key can be compromised either by physical extraction from a captured node or by breach in security protocol. The denial of service attack renders a node by overloading it with unnecessary operations and communication and may be able to make the whole distributed computing system inoperable. Coremelt attacks can target communication links blocking the exchange of useful information and results traffic congestion in broadcast network. Replay attack allows an attacker to record messages at one instance and replay it later at different locations. There are other possibilities of different types of attacks on multicast such as blackhole, jellyfish, neighbor and rushing attack. There are risks of snooping, phishing, cross site scripting, distributed denial of service, unauthenticated request forgery, authenticated request forgery, intranet request forgery and exploitation of distribution on web enabled broadcasting system such as digital TV [24]. The basic objective of the threat analytics is to assess risks of different types of malicious attacks and explore risk mitigation plans accordingly.

Theorem 2: **ASBA explores different scenarios of broadcast corruption in terms of agents (broadcaster, recipients, system administrator), data, communication channel, broadcast mechanism and system.**

Model checking is an automated technique for verifying a finite state concurrent system. It represents a system by automata, represents the property of a system by logic and designs model checking algorithm accordingly. The basic objective of verification or model checking algorithm of ASBM is to ensure secure group communication of a broadcasting system. It provides one or more security services by detecting, preventing or recovering from one or more threats.

Model Checking Algorithm (MCA1):

Objectives: (a) Primary: Automated system verification; (b) Secondary: Semi-automated system verification based on agent's feedback;

1. Detect symptoms of threats on broadcasting system. Do data mining on broadcasting system parameters. Call table 1 on threat analytics.
2. Assess risks of single or multiple threats on broadcasting system.
3. Mitigate risks by exploring strategic moves and action plans.

4. Evaluate and monitor security intelligence and revelation principle in real-time.

SL No.	Symptoms of corruption	Parameters for data mining	Action plans
1.1	Broadcaster or service provider or sending agent	Sybil identities, alerts from the recipients and system administrator, role, responsibilities and performance;	Audit authenticity, authorization, correct identity, honesty and accountability of broadcaster; check legal or regulatory compliance policy; lodge complains to system administrator.
1.2.	System administrator	Sybil identities, alerts from the recipients and broadcaster, responsibilities, performance and efficiency of administration;	Check regulatory compliance, switching of service, boycott of service, mass protest at high level.
1.3	Receiving agents or service consumers	(a) Privacy : group, forward and backward; (b) collusion in secret sharing; (c) sybil identities, (d) node replication, (e) node deletion.	Check access control policy of recipients; key generation and distribution policy; analyze feedback of neighbors; verify e-passport or trusted explicit and implicit certification of sensor nodes; do resource testing; call challenge response protocol for node attestation verification.
2.0	Data corruption	(a) False data injection attack, (b) Shilling attack: ad slot allocation, content of adwords: fraudulent recommendation, exposure time and frequency, customization, delivery, click rate, impression.	(a) Audit fairness, correctness, integrity, non-repudiation, confidentiality, trust, accountability and transparency of broadcast data. (b) Evaluate honesty and trust worthiness of recommender system.
3.0	Communication network corruption	(a) Wormhole, coremelt, blackhole, jellyfish, rushing and neighbor attacks : traffic congestion, delay, packet loss, work load, bandwidth and channel capacity; (b) web security; (c) network topology; (d) viral attack.	(a) Audit network traffic, (b) Check the risks of snooping, hacking, phishing, cross site request forgery and scripting, session hijack for service oriented computing (SOC) platform. (c) call anti-virus software adaptively.
4.0	Broadcast mechanism corruption	(a) Broadcast schedule : logic, delay and excepting handling strategy; (b) malicious business intelligence; (c) QoS : denial of service (DoS), network connectivity, internet speed, noisy signal, data loss, data integrity, call drop and disruption in energy supply,	(a) Rectify scheduling errors, consolidation of requests; collaboration in rescheduling and exception handling; (b) verify commitment, transparency and accountability in payment mechanism: violations in contract between S and R *or* error in payment function computation *or* error in channel and package configuration *or* flaws in pricing algorithm, audit computational intelligence of pricing of stocks and derivatives; (c) audit Total Quality Management (TQM) policy.
5.0	System schema :computing, data,application and networking	(b) System performance: workflow, safety, reliability, consistency, liveness, deadlock freeness, synchronization and reachability.	Audit computational intelligence, interfaces and snags in application integration; review plan for regular, preventive and breakdown maintenance.

Table 1 : Threat Analytics for Broadcasting System Verification

In ASBM, corruption may occur in various ways. The first scenario is related to corrupted sender and honest recipients; the sending agent is compromised by an adversary and broadcasts false data to the recipients; the corrupted sender gets payment from the adversary. The second scenario is associated with honest sender and corrupted recipients; the sending agent is an honest, rational and fair player and broadcasts correct message. But, several recipients are compromised by the adversary. It can be direct or indirect attack. In case of direct attack, the malicious agents get the decryption keys from the corrupted recipients and intercept the secret message directly. In case of indirect attack, several corrupted recipients receive the secret message and disclose the same to the adversary. The third scenario is related to corrupted sender and corrupted recipients where both the sender and some recipients are compromised. The fourth scenario is associated with corrupted communication channel; the malicious adversary can capture the secret data directly from the communication channel though the sender and the recipients are not corrupted. Theorem 6 is focused on corrupted communication channels. Alternatively, the adversary may delay the flow of data by creating congestion in the communication network. In worst case, both the sender and the recipients are corrupted and the channel is unsecured. Theorem 7 is focused on data corruption and also the corruption of the sender and system administrator.
Adversarial model : The adversary is capable of corrupting a set of recipients so that A can access to the keys of the corrupted players. The corruption strategy indicates when and how parties are corrupted. In case of static corruption model, the adversary is given a fixed set of parties whom it controls. Honest parties remain honest throughout and corrupted parties remain corrupted. In case of adaptive corruption model, adaptive adversaries are given the capability of corrupting parties during the computation. The choice of who to corrupt, and when, can be arbitrarily decided by the adversary and may depend on its view of the execution.
A broadcast protocol allows a sender to distribute a secret through a point-to-point network to a set of recipients such that (i) all recipients get the same data even if the sender is corrupted and (ii) it is the sender's data if it is honest. Broadcast protocols satisfying these properties are known to exist if and only if $t < n/3$, where n denotes the total number of parties, and t denotes the maximal number of corruptions [11]. When a setup allowing signatures is available to the parties, then such protocols exist even for $t < n$. A recent work in [5] argues that the communication model adopted by [4] is unrealistically pessimistic. The problem of adaptively secure broadcast in a synchronous model is possible for an arbitrary number of corruptions. A broadcast encryption scheme allocates keys to the recipients for a subset of S of U, the center can broadcast messages to all users where all members of S have a common key. [17] introduces a parameter 'resiliency' that represents the number of users that have to collude so as to break the broadcasting security scheme. The scheme is considered broken if a recipient that does not belong to the privileged class can read the secret. A scheme is called k-resilient if it is resilient to any set of size k. ASBM results correct and fair output if and only if all the agents (S, A and R), communication channel, broadcast data, broadcast mechanism and payment function are free of corruptions. The following test cases 1-18 justify this claim.
[Test Case 1 : Corrupted Broadcaster or Sending Agent]: The recipients must verify the consistency, correctness and fairness of broadcasted data in real time. A broadcasting agent may be corrupted. In other case, the broadcaster is honest but the source of data is dishonest. For example, the results of election or voting are broadcasted differently though different broadcast channels at the same time. It is possible for the recipients to detect the inconsistency and incorrectness of broadcasted data by comparing the mismatch among different channels. The recipients may doubt the false image or photo taken surprisingly during a terror attack or war. In case of auction, it is a serious issue if the broadcaster is corrupted since it is difficult to identify the flaws and inconsistencies in broadcast if the recipients preserve the privacy of broadcast and there is no information exchange among the recipients.
[Test Case 2 : Corrupted Recipients]: The receiving agents may be corrupted in many ways. A recipient may disclose private broadcasted data to the adversary or there may be collusion among the recipients or there may be a sybil entity of one or more recipients in the broadcasting system. These issues have been discussed in existing works in details through verifiable secret sharing schemes. For example, a corrupted recipient can submit false bid to confuse the other bidders in an auction or reverse auction mechanism. It is essential to verify the abnormality and noisy data submitted by the bidders in each round of bidding.

[Test Case 3 : Corrupted System Administrator] The honest agents are expected to boycott the fraudulent broadcast and should adopt the strategic move of mass protest to the highest authority of information and communication system if the broadcast forum is idle and not responsive against corruption.

Theorem 3: ASBM must audit any violation in broadcast plan. A corrupted communication channel is a real threat to a web enabled broadcasting system; another threat is wormhole attack.

[MCA2] *Threats* : (a) broadcast plan violation, (b) web security, (c) wormhole attack;
Objective: (a) Semi-automated system verification (b,c) Automated system verification;
Risk assessment : (a) Sense flaws in broadcast plan: delay, cancellation, scheduling logic, exception handling and strategic moves; (b) detect web security attacks (e.g. snooping, phishing, session hijack); (c) detect the risk of wormhole attack.
Risk mitigation: (a) collaborative planning in exception handling, cancelation and rescheduling; sense-and-respond adaptive planning in broadcast scheduling; (b) real-time monitoring of web traffic and security schema; (c) detect wormhole attack using packet leashes.

[Test Case 4: Web Attack] The model checking algorithms must verify a set of critical parameters such as the risk of snooping and phishing, validation of service oriented computing schema in terms of logic, main flow, sub flows and exception flows of the application, cross site scripting, injection flaws, malicious file injection by testing application programming interfaces and code, insecure direct object reference, cross site request forgery, information leakage and improper error handling, broken authentication and session hijack, insecure cryptographic storage and failure to restrict URL access [25,26,27].

[Test Case 5: Wormhole Attack] A *wormhole* attacker records packets at one point in adhoc wireless communication network, tunnels the packets possibly selectively to another point and retransmits them there into the network. The attacker may not compromise any hosts and even if all communication protocols provide authenticity and confidentiality correctly. Packet leashes may be used for detecting and defending against wormhole attacks. A leash is any information that is attached with a packet to restrict its maximum allowed transmission distance. A geographical leash ensures that the recipient of the packet is within a certain distance from the sending agent. A temporal leash ensures that the packet has an upper bound on its lifetime which restricts the maximum travel distance.

Theorem 4: ASBM must audit group, forward and backward privacy for a dynamic broadcast group.

[MCA3] *Threat* : Insecure group communication;
Objective : Semi-automated system verification by system administrator;
Risk assessment : Sense violation in group, forward and backward privacy.
Risk mitigation: (a) verify the efficiency of key update protocols for join, leave, subgroup change, merge and split in a dynamic broadcast network. (b) Audit revelation principle.

[Test case 6: Privacy in adaptively secure braodcast] Key Update is a set of protocols that update the signcryption and unsigncryption keys to preserve group, forward and backward privacy and key independence [7,8]. Group key privacy guarantees that it is computationally infeasible for a passive adversary to discover any group key. Key independence guarantees that a passive adversary who knows any proper subset of group keys cannot discover any other group key not included in the subset. To prevent the recipients who have already left from accessing future communications of a group, all keys along the path from the leaving point to the root node of the key tree are to be changed. In case of a change of subgroup within a group, only old subgroup key is replaced with a new subgroup key. It ensures forward privacy. To prevent a new recipient from accessing past communications, all keys along

the path from the joining point to the root node of the key tree are changed. In case of a change of subgroup within a group, only old subgroup key is replaced with a new subgroup key. It ensures backward privacy.
Adaptive key refreshment management is associated with various types of events of a broadcasting system such as join, leave, split, merge and change of subgroup of the recipients [7; see section 3.3 for details]. When a recipient wants to *join* the broadcasting group, the group controller authenticates the new member by distributing a group key, a subgroup key and an individual key. *Leave* protocol is called when a recipient wants to leave permanently from the group. A recipient may *change its subgroup* and join a new subgroup leaving from the old subgroup. *Merge* protocol is called when several recipients merge together to form a new sub-group. *Split* protocol is called when several recipients want to break a merger and split.

Theorem 5: It is essential for ASBM to monitor traffic congestion and QoS in real-time to mitigate coremelt, blackhole, jellyfish, rushing and neighbor attack.

[MCA4] *Threats* : (a) coremelt, (b) blackhole, (c) jellyfish, (d) rushing and (e) neighbor attack;
Objective : (a,b,c,d) automated system verification (e) semi-automated system verification;
Risk assessment: (a) coremelt: sense network congestion; (b) blackhole: sense data loss during broadcast; (c) jellyfish: sense delay in broadcast, (d) rushing: sense fast broadcast and synchronization problems, (e) neighbor: detect false feedback from neighbors, detect collusion of neighbors;
Risk mitigation: do real-time traffic monitoring; (a) coremelt: identify target links and sources of traffic congestion and excessive load; (b) blackhole: identify missing data and complain to the broadcaster, (c) jellyfish: intrusion detection; (d) neighbor: identify malicious neighbors; call antivirus software against viral attacks. (e) rushing attack: the receiving agents give alert to the broadcaster about timing problem.

[Test Case 7: Coremelt Attack] The malicious attackers send traffic between each other and not towards a victim host in coremelt attack. It is a powerful attack since there are $O(n^2)$ connections among n attackers which can cause significant congestion in core network. Broadcast networks often use web service to enable coordination among physical systems. The malicious attackers are able to flood the end hosts with unwanted traffic to interrupt the normal communication. This is a specific type of Denial-of-Service (DoS) attack where the network link to system server is congested with illegitimate traffic such that legitimate traffic experiences high loss and poor communication performance. Such a poor connectivity can damage critical infrastructure with cascading effect. There are three steps to launch a coremelt attack [28]. First, the attackers select a link in the communication network as the target link. Then, they identify what pairs of nodes can generate traffic that traverses the target link. Finally, they send traffic between the identified pairs to overload the target link. Thus, the attacker uses a collection of nodes sending data to each other to flood and disable a network link. To address such attacks, it is important to identify the source of excessive traffic and prioritize legitimate traffic.

[Test Case 8: Blackhole, Jellyfish & Neighborhood Attack] A blackhole attacking agent tries to intercept data packets of the multicast session and then drops some or all data packets it receives instead of forwarding the same to the next node of the routing path and results very low packet delivery ratio. A jellyfish attacker intrudes into the multicast forwarding group and delays data packets unnecessarily and results high end-to-end delay and degrades the performance of real-time application. A neighborhood attacking agent forwards a packet without recording its ID in the packet resulting a disrupted route where two nodes believe that they are neighbors though actually they are not. Rushing attack exploits duplicate suppression mechanisms by forwarding route discovery packets very fast.
The broadcasting system requires an efficient network traffic monitoring system to avoid these attacks. A broadcaster seeks to minimize own delay of data communication and the malicious agents seek to maximize the average delay experienced by the rational players. Congestion is a critical issue in both wired and wireless communication channel. The broadcaster should monitor the congestion in communication channel in real time so that all the recipients receive the data stream in time without any loss of data or delay. The critical issue in congestion control and quality of service in adaptively secure

broadcast is data traffic [1]. Congestion occurs in a communication channel if the load on the channel is greater than the capacity of the channel. It is measured in terms of average data rate (= data flow / time). Congestion control measures the performance of the broadcast channel in terms of delay and throughput. Delay is the sum of propagation and processing delay. Delay is low when load is much less than capacity. Delay increases sharply when load reaches network capacity. Throughput is the number of data packets passing through the network in unit time. The quality of service should be measured in terms of reliability, delay, jitter and bandwidth.

Theorem 6: The recipients must verify the correctness and consistency of broadcast data to detect false data injection, replay and shilling attack in ASBM.

[MCA5] *Threats:* False data injection attack, shilling attack, replay attack;
Objective : Semi-automated system verification;
Risk assessment: (a) Sense incorrect, fraudulent and false broadcast, flaws in data visualization and statistical errors through logical and analytical reasoning. (b) Detect the risk of shilling attack in digital adwords : push and nuke attacks.
Risk mitigation: (a) Audit revelation principle and validate quality of statistics; check consistency and rationality of broadcast. (b) Verify fairness, correctness and trust in recommender system performance. (c) Identify sources of data corruption. (d) Reject false data broadcast, complain to the broadcast forum and impose penalty in payment function.

False data injection attack broadcasts incomplete, corrupted, noisy, got-up and incorrect data through intrusion of malicious agents or corrupted sending agent and affects the reliability of the broadcasting system. The receiving agents and the system administrator must verify the fairness, trust and correctness of broadcasted data in time.

[Test case 9 : Corrupted Digital or Internet TV Broadcast] : Today, false data injection attack is a very common threat to dull TV broadcast in the form of got-up game fixed by the betting world, fraudulent budget session, unethical fake low impact non-investigative journalism and cultural shock in vulgar music, films, dramas and reality shows. Old telecasts are often broadcasted as live telecasts through *replay attack* [e.g. telecast of football and cricket matches through popular sports channel]. In this case, the sender i.e. the broadcaster is not corrupted, the recipients or viewers of the broadcasted data are also honest and innocent. But, the sources of broadcast data are corrupted. The threat of false data injection attack should be mitigated through rational social choice. The verification mechanisms require the intervention of trusted third parties or detectives who should arrest the malicious agents (e.g. betting agencies). The recipients must adopt tit-for-tat strategy: honest public campaign against fake shows, boycott got-up broadcast, threats and punishments against corrupted players, teams and associations, financial audit, verification of fairness, correctness and transparency in event management policies. The players must be honest, ethical and professional in their actions, behaviors, practice and attitude. The recipients must verify the quality of broadcast and provide true, honest and intelligent feedback to the broadcasting forum. If the forum is inactive, toothless, clawless and casual, the deceived agents should report to the highest authorities and seek for legal help to corporate governance. The recipients may adopt retaliative moves such as rejection of fraud channels or switching from one service provider to the other for better quality of service.

It is essential to design a broadcast performance scorecard based on a set of performance metrics and rating scale [1-5; 1: very dissatisfied, 2: dissatisfied, 3: neither satisfied nor dissatisfied or neutral, 4: satisfied, 5: very satisfied]. But, there are issues of trust, reliability, acceptability, transparency and correctness in research methodology and function of broadcast audience research council. The recommender system may be biased and controlled by industrial bodies. The recipients or the viewers may be shown false rating and ranking of different channels. It is really hard to detect whether the system administrators and regulators are compromised by the adversaries. It is also critical to collect

honest feedback from the experts regarding the performance of various broadcasting channels. It is a hard problem which should be resolved jointly through secure multi-party computation and social choice.

[Test case 10 : Digital media the challenges ahead] Adaptively secure broadcast is a great challenge for the future of impartial, independent and accurate world news coverage. The future of world news coverage is a burning issue to balance of power in multi-polar world. Can the viewers trust joint broadcast in global news coverage? What is the responsible role of media at a time of global conflict? What is the coordination mechanisms in global media broadcast? Do online players pose a threat? Is offline media facing threats from online one? What is the importance of news in the time of Internet; should there be a fair competition among different media channels? Should the media be selective in coverage? Responsive and investigative reporting is a challenge. Do media need to be responsible against domestic influence i.e. the pressure from national government? What should be the focus of world coverage: the impact on policy, global perspectives and domestic coverage, boundaries between reporting and dictating policy, the responsibility being a world media house, media's role in galvanizing opinion. When should media act as a cheerleader? Can government run media house be more objective? What are the responsible roles of govt. run media house and editorial forum? Are global media houses really objective? Freedom of state run media is a debatable issue. Can broad level of freedom of expression inject false data massively to the viewers? Does state funding blur editorial freedom; state run media as cultural mouthpieces; impartiality and objectivity possible at the same time? Should the global media houses be neutral? What should be corporate social responsibilities of media? Who polices the global media and how? A good story makes huge difference; can the government made media house be unbiased? How to detect whether the coverage is unbiased or biased controlled by the government? How to call out biased global coverage? Funding is an issue; there are challenges of working against threats from power centres; The pressure of being an influential voice is really hard. There are other several critical issues : rise of social and digital media today; the threat of traditional media today and challenges from social and online media; does digital media threaten conventional media? Can TV channels compete with social media?

[Test case 11 : False Data Injection Attack in Corporate Governance]: Nowadays, the common public, entrepreneurs and investors don't believe in statistics or data mining or super flop leadership; they don't trust statistics. They have lost their faith in statistical jugglery through so called popular cheap broadcasts. For example, who is verifying the correctness and fairness of following statistics broadcasted by Govt. of State A of country X in the context of a business summit?

- Gross value added growth in 2014-15: State A – 10.48%; Country X - 7.5 %!
- Increase in per capita income in 2014-15: State A - 12.84%; Country X - 6.1.%!
- Increase in industry in 2014-15: State A - 8.34%; Country X - 5.6%!
- Increase in agriculture, forestry and fishery in 2014-15: State A - 6.49%; Country X - 1.1%.
- Starting of projects of Rs. 91000 crores!
- Attracting investment proposals of $37 billions or Rs. 250104 crores through MOUs, Rs. 116958 crores in manufacturing sector.
- Noisy false data in announcement of budget fund allocation

[Test case 12] : A news channels broadcast the exaggerated images of natural disaster (e.g. flood, cyclones, storm, snowfall, earthquake) for a state B of country Y; horrible situations are created artificially by cutting of energy and utility supply, disruption in food supply chain management and closing bank operations. The government of state B claims huge amount of false demand on account of losses and damages from the central government of country Y through such corrupted broadcast. The other objective is to maximize the number of telephone calls by creating panic among the near and dear ones of the residents of the victimized places.

Test Case 13 (Misleading Corporate Communication) : Due to the successful execution of its business continuity plan which largely mitigate the financial impact of heavy downpour and flooding in city C, an IT firm Z has reaffirmed that it expects to achieve its previously announced full year guidance

of at least $12.41 billion and its non GAAP diluted EPS guidance of at least $3.03. How? What are the revenue optimization strategies? The other IT firms have already announced revenue warning for the current financial year. It is possible to detect the inconsistency and vagueness in corporate communication by comparing the trends in the industry.

[Test case 14 : Digital Advertising] : Malicious broadcast is a real threat to the digital advertising world and financial service sector. If the recipients sense flaws in digital advertising, the system administrator must verify the correctness, fairness and transparency of the system through analytics on ad slot allocation, content of adwords, exposure time and frequency, customization, delivery, click rate, and impression. Today's broadcast is closely associated with advertising as a recommender system. But, there is risk of *shilling attack* in the form of *push* and *nuke* attacks where the rating of target items are increased and lowered successively. The advertising world may be digitally divided with a flavor of revenge and retaliation due to zero or low investment on advertising by the corporate world. A corrupted broadcasting system may be involved in brand dilution of a good company through baseless, mischievous and false propaganda. Alternatively, the broadcasting system can push a set of targeted items of poor quality and brand to the public through fraudulent adwords, euphemism and attractive presentation of the popular brand ambassadors. But after the disclosure of the information on such types of malicious attacks, the recipients may lose their trust in the adwords of the digital world in future.
The financial service sector (e.g. stock market) may be also threatened by malicious business intelligence. Real-time correct financial market information is expected to be broadcasted to a large number of recipients. But, incorrect broadcast may result huge financial loss in stock and derivatives market. This is the most dangerous threat on a broadcasting system where the sender and the recipients may be honest but the sources of broadcasted data are corrupted. The recipients must threaten and refuse false adwords and complain to the broadcasting forum, quality control and detective agencies and government authorities in time against fraudulent business intelligence. The profiles of shilling attackers must be deleted with the help of collaborative filtering and efficient ranking system. The problem should be solved through regulatory compliance (e.g. RTI, consumer protection acts), cryptology and network security jointly.

Theorem 7: ASBM must call efficient and intelligent tracing mechanisms to detect sybil, node replication and node deletion attack.

[MCA6] *Threats* : Sybil attack, node deletion attack, node replication attack.
Objective : automated system verification;
Risk assessment : Analyze feedback from neighboring nodes of a sensor network. Sense sybil, node replication and node deletion attack.
Risk mitigation:
Input : A self-set S $\subseteq$ U, a monitoring set M $\subseteq$ U.
*Output: f*or each element $m \in M$, either self or non-self / danger or normal;
Move 1:
$D \leftarrow$ set of detectors that do not match any $s \in S$.
for each $m \in M$ do
check e-passport;
if *m* matches any detector $d \in D$ then identify m as non-self;
else identify m as self;
Move 2 :
for each $d \in D$ do
monitor a set of m $\leftarrow$ check resource capacity: computing, storage and communication schema;
monitor *feedback* of neighboring nodes;
detect danger signal and identify suspicious nodes M';
for each $m' \in M'$ do
if m' provides invalid e-passport then identify m' as danger nodes;
else identify m' as normal node;

check if non-self or suspicious node is benign or malign danger node;
if it is malign then kill it else give alert.

[Test Case 15 : Sybil and Node Replication Attack] It is really complex to trace the corrupted players in the broadcast. A broadcasting communication network is defined by a set of entities, a broadcast communication cloud and a set of pipes connecting the entities to the communication cloud. The entities can be partitioned into two subsets: correct and faulty. Each correct entity presents one legitimate identity to other entities of the distributed system. Each faulty entity presents one legitimate identity and one or more counterfeit identities to the other entities. Each identity is an informational abstract representation of an entity that persists across multiple communication events. The entities communicate through messages. A malicious agent may control multiple pseudonymous identities and can manipulate, disrupt or corrupt a distributed computing application that relies on redundancy by injecting false data or suppressing critical data it is sybil attack [29]. The sybil, node replication and node deletion attacks may be detected through intelligent tracing mechanism as discussed in the following section.
There are various types of tracing mechanisms against sybil attack: trusted explicit and implicit certification, robust authentication, resource testing and incentive based game [30]. In case of trusted certification, a centralized authority assigns a unique identity to each entity. The centralized authority verifies computing, storage and bandwidth capability of the entities associated with the broadcasting system on periodic basis. The recipients validate the received data from the sender and checks logically whether there is any inconsistency or chance of injection of false data in the decrypted message. Another approach of tracing is to adopt incentive based game wherein the objective of the detective is to compute the optimum possible reward that reveals the identity of maximum number of corrupted agents [24]. A local identity (l) accepts the identity (i) of an entity (e) if e presents i successfully to l. An entity may validate the identity of another identity through a trusted agency or other entities or by itself directly. In the absence of a trusted authority, an entity may directly validate the identities of other entities or it may accept identities vouched by other accepted entities. The system must ensure that distinct identities refer to distinct entities. An entity can validate the identity of other entities directly through the verification of communication, storage and computation capabilities. In case of indirect identity validation, an entity may validate a set of identities which have been verified by a sufficient count of other identities that it has already accepted.

[Test Case 16 : Sensor Node Corruption] Sensor node attestation verification is a critical requirement of a smart broadcasting system : check if a sensor node is tampered by an adversary; check the configuration and correct setting of each sensor node; detect whether malicious software is loaded into sensor nodes; verify the integrity of the code; perform secure code updates and ensure untampered execution of code [31]. Each node should be attested with a valid digital test certificate. The verification algorithm must verify the identity and tampering status of each node. The basic objective of device attestation is that a malicious agent should not be able to configure or change correct setting of each node. A challenge response protocol is employed between a trusted external verifier and a sensor node.

Theorem 8: **ASBM must audit malicious financial intelligence on payment function and transparency of payment mechanism.**

[MCA7] *Threat* : Malicious financial intelligence;
Objective : Periodic audit;
Risk assessment : (a) Sense violation in contractual clauses between S and R on payment function, payment mechanism and payment mode. (b) Sense poor QoS : technical snags and the negative social impact of broadcast.
Risk mitigation : (a) Audit fairness and correctness of computation on payment function; (b) check error in channel and package configuration; (c) check flaws in pricing algorithm; (d) verify transparency of payment mechanism; (e) Audit broadcasting system performance and QoS; do root cause and pareto

analysis on technical snags like problems of data, audio and video image quality, noise, inconsistency, connectivity problem during natural disaster and power cut; (e) revise maintenance plans and disaster management plan to improve resiliency of broadcast system; (f) promote innovation in program design and implement total quality management (TQM) policy.

[Test Case 17 : Corrupted Payment Function and Payment Mechanism] The payment function should be designed innovatively, fairly and rationally in terms of intelligent contract, pricing strategy, payment terms, incentives and penalty function. The payment function is negotiated through various ways such as auction, combinatorial auction, discriminatory price ladder, swing option, choice of payment terms and mode, price change and price protection strategies. Generally, the broadcasting entity and the recipients are supposed to act cooperatively. The broadcaster communicates the secret data to the recipients who decrypt the encrypted data, validate it and pay to the broadcaster. This is a fair and rational business scenario. But in case of malicious attack, one or more players may be corrupted and act non-cooperatively. They disclose the secret data or the decryption keys to the adversary. The corrupted agents may be the sender or recipients. In case of corruption, the corrupted agents receive the payment from the adversary. Alternatively, the broadcaster computes payment function dishonestly through flawed package configuration and price protection. The malicious business intelligence is also associated with the flaws in broadcasting scheduling: delay in schedule, error in scheduling logic, exception handling error and replay attack. It is essential to audit malicious business intelligence by verifying transparency and accountability of the payment mechanism and negotiated broadcast plan from the perspectives of violation in contractual clauses among the agents, flaws in payment function computation or pricing algorithm, channel and package configuration and commitment.

3.2 Communication Complexity

Theorem 9: The cost of communication for SSMR model is O(n) where n is number of agents involved in the broadcast. It also depends on strategic moves of broadcast communication.

The broadcasting system administrator may adopt different types of communication models depending on the requirements of an application such as one-to-many or single sender multiple receivers (SSMR), many-to-one or multiple senders single receivers (MSSR) and many-to-many or multiple senders multiple receivers (MSMR) communication models. In a three party model a sending agent, multiple receiving agents and a system administrator are associated with the broadcasting system. In a bi-party model, a sending agent and multiple receiving agents operate without the support of any administrator. The topology of the broadcast communication network may be static or dynamic. In a static network, the number of agents is constant and the topology is also fixed. In a dynamic network, the number of agents change with time internally through change of subgroups within a group or merge or split operations or externally through join and leave operations [13,14]. The topology is not fixed with time. The sending agent i.e. the broadcaster generally sends a data stream or a set of data packets to the receiving agents through a secure communication channel. Alternatively, the broadcast may not be a private communication. The communication signal may be digital or analog. In case of SSMR model, the cost of communication is O(n) where n is the number of agents associated with the broadcasting system. In case of MSMR model the cost of communication may be $O(n^2)$. The communication complexity also depends on the intelligence of broadcast plan, number of communication rounds of a broadcast session, message length, complexity of data stream and network congestion.

The next critical issue is broadcast mechanism or multicast communication protocol. The receiving agents exchange their demand plans to the sending agent. The agents jointly settle broadcast plan (P_b) and payment function (p_f) through collaborative planning, forecasting, negotiation and exception handling. The sending agent (S) selects a set of strategic moves for intelligent communication. S consolidates the communication load requested by the receiving agents. S selects an efficient scheduling logic for adaptively secure broadcast: FIFO, LIFO, priority queue and data filtering. ASBM does not require any time synchronization between the sender and the recipients; the data stream is broadcasted as per negotiated broadcast plan. The data stream may be filtered and multicasted to different sub-groups within a broadcasting group. S may send data in a single round or multiple rounds in case of multi-party

negotiation. The sending agent communicates with the receiving agents through unidirectional or bidirectional or synchronous or asynchronous mode. S tries to explore an intelligent broadcast plan by solving a single or multi-objective optimization problem minimizing maximum response time, number of requests meeting the deadline, the sum of response time and optimizing revenue subject to various constraints like time deadline and budget of the receiving agents and target profit margin of the broadcasting agent. In case of private broadcast, S encrypts or signcrypts or signs the broadcasted data with digital signature and sends the private data through a secure communication channel. S may also adopt privacy preserving data mining (ppdm) algorithms. The receiving agents decrypt or unsigncrypt the received data and verifies security intelligence of the broadcasting mechanism.

3.3 Computational Intelligence

Theorem 10 : The cost of computation of ASBM is a function of the complexity and efficiency of security algorithms, automated system verification algorithms and broadcast plan.

The computational complexity is a combinatorial issue for ASBM. The most critical issue is the cost of computation of security algorithms. The computational burden also depends on key management strategies, broadcast scheduling algorithm, model checking algorithms, payment and penalty computation. The cost of broadcast scheduling algorithm depends on the complexity of optimization problem: single objective or multiple objectives function, number of constraints and scheduling logic [15,16]. The cost of payment function depends on the complexity of discriminatory pricing algorithm, package configuration and incentives. The cost of model checking algorithm is a function of the complexity of threat analytics, risk assessment and mitigation plans.

A broadcast encryption scheme (BE) is a set of algorithms: KeyGen, Signcrypt, Unsigncrypt and Keyupdate [17]. Secure communication is one of the most critical issues of broadcasting system; cryptography ensures privacy and secrecy of sensitive data through encryption method. S encrypts a message (m) with encryption key and sends the cipher text (c) to the recipients (R). R transforms c into m by decryption using secret decryption key. An adversary may get c but cannot derive any information. R should be able to check whether m is modified during transmission. R should be able to verify the origin of m. S should not be able to deny the communication of m. There are two types of key based algorithms: symmetric and public key. Symmetric key encryption scheme provides secure communication for a pair of communication partners; the sender and the receiver agree on a key k which should be kept secret. In most cases, the encryption and decryption keys are same. Secure broadcast authentication is hard with symmetric encryption key with untrusted recipients. In case of asymmetric or public-key algorithms, the key used for encryption (public key) is different from the key used for decryption (private key). The decryption key cannot be calculated from the encryption key at least in any reasonable amount of time. Asymmetric RSA encryption achieves broadcast authentication where each recipient can verify the authenticity of received data but can not generate authentic messages.

A *digital signature* is a cryptographic primitive by which a sender (S) can electronically sign a message and the receiver (R) can verify the signature electronically. S informs his public key to R and owns a private key. S signs a message with its private key. R uses the public key of S to prove that the message is signed by S. The digital signature can verify the authenticity of S as the sender of the message. A digital signature needs a public key system. A cryptosystem uses the private and public key of R. But, a digital signature uses the private and public key of S. A digital signature scheme consists of various attributes such as a plaintext message space, a signature space, a signing key space, an efficient key generation algorithm, an efficient signing algorithm and an efficient verification algorithm. Digital signature provides authentication and non-repudiation through asymmetric property of cryptography at high cost of computation and communication. One way hash function may be used as the basic building block of asymmetric RSA digital signature and cryptographic commitment. A one-way function is a function that is easy to compute but computationally infeasible to invert. If x is a random string of length k bits and F is a one-way function then *F* can be computed in polynomial time as y = F(x) but it is almost always computationally infeasible to find x' such that F(x') = *y.* Merkle hash tree is an efficient construction of one way function [18].

Another alternative interesting option for secure broadcast authentication is signcryption. Traditional signature-then-encryption is a two step approach. At the sending end, the sender signs the message using a digital signature and then encrypts the message. The receiver decrypts the cipher text and verifies the signature. The cost for delivering a message is the sum of the cost of digital signature and the cost of encryption. Signcryption is a public key primitive that fulfills the functions of digital signature and public key encryption in a logically single step and the cost of delivering a signcrypted message is significantly less than the cost of signature-then-encryption approach [19,20]. A broadcasting system is vulnerable to insecure communication. The basic objective is that the system properly signcrypts all sensitive data. A pair of polynomial time algorithms (S,U) are involved in signcryption scheme where S is called signcryption algorithm and U is unsigncryption algorithm. The algorithm S signcrypts a message m and outputs a signcrypted text c. The algorithm U unsigncrypts c and recovers the message unambiguously. (S,U) fulfill simultaneously the properties of a secure encryption scheme and a digital signature scheme in terms of confidentiality, unforgeability and nonrepudiation. *Signcryption* can ensure efficient secure broadcast communication. Alternatively, the broadcaster may adopt different types of privacy preserving data mining (PPDM) strategies such as randomization, summarization, aggregation, generalization, suppression, de-identification and k-anonymity. Intelligent PPDM strategies may improve the cost of computation in secure broadcast. The basic objective is to provide confidentiality, data integrity, authentication and non-repudiation in the communication of sensitive data.

Key update **:** ASBM adopts adaptive key refreshment protocols to preserve group, forward and backward privacy for join, leave, subgroup change, merge and split. *Key Update* is a set of protocols that update the signcryption and unsigncryption keys to preserve group, forward and backward privacy and key independence [7,8]. The efficiency of the proposed broadcast key management is evaluated in terms of key storage, encryption, decryption and communication overhead. The basic objective of adaptive key construction is to improve the efficiency of broadcast by reducing the cost of different overheads. There are three different approaches of key management: centralized, decentralized and distributed [8]. In case of centralized approach, a single entity acts as a group controller. But, the central controller is a single point of failure; the entire group will be affected if there is a problem with the controller. In the decentralized approach, a set of subgroup controllers are used to manage change of membership of each subgroup locally. In case of distributed key management approach, there is no group controller. The group key can be either generated in a contributory way or generated by a member. All the members may participate in access control and generation of group key. The cost of computation and communication is a function of group size, number of subgroups, number of tiers in the key tree and number of keys to be stored by each recipient. Let us explain key update operation for secure broadcast in a dynamic group through an example.

Test case 18 : *Key management protocols for secure broadcast for a dynamic group*
Let us consider following combinatorial reverse auction model.

- A group of recipients or receiving agents : S_1, S_2,...,S_9 ; S_1 and S_2 merge together.
- A set of data to be sent by a broadcasting agent B : i_1,i_2,i_3
- A set of division set or bundle: (i_1,i_2),(i_1,i_2,i_3) and (i_3).
- A set of subgroups of the recipients for the first broadcast cycle: sg_1(S_1, S_2, S_3), sg_2(S_4, S_5, S_6) and sg_3 (S_7,S_8, S_9); these three subgroups are competing over the item sets (i_1,i_2), (i_1,i_2,i_3) and (i_3) respectively.
- A set of winners for the first broadcasting cycle: S_3,S_6, S_8 over the item sets (i_1,i_2), (i_1,i_2,i_3) and (i_2,i_3) respectively.
- $K_{1\text{-}9}$ is the group key (K_g) shared by all the recipients. B can send common private message to all the recipients of the group encrypting the message with this group key.
- K_{123}, K_{456}, K_{789} are subgroup keys of the sub groups sg_1 (S_1,S_2, S_3), sg_2 (S_4,S_5, S_6) and sg_3 (S_7,S_8, S_9) respectively. B can send a private message to a subgroup encrypting with the relevant subgroup key. The privacy of a subgroup is protected through subgroup key.

- K_1, …,K_9 are individual keys of the recipients S_1,S_2,…,S_9 respectively. B sends a private message to a recipient by encrypting the individual key. The distribution of symmetric keys for secure group communication has been shown in figure 1.

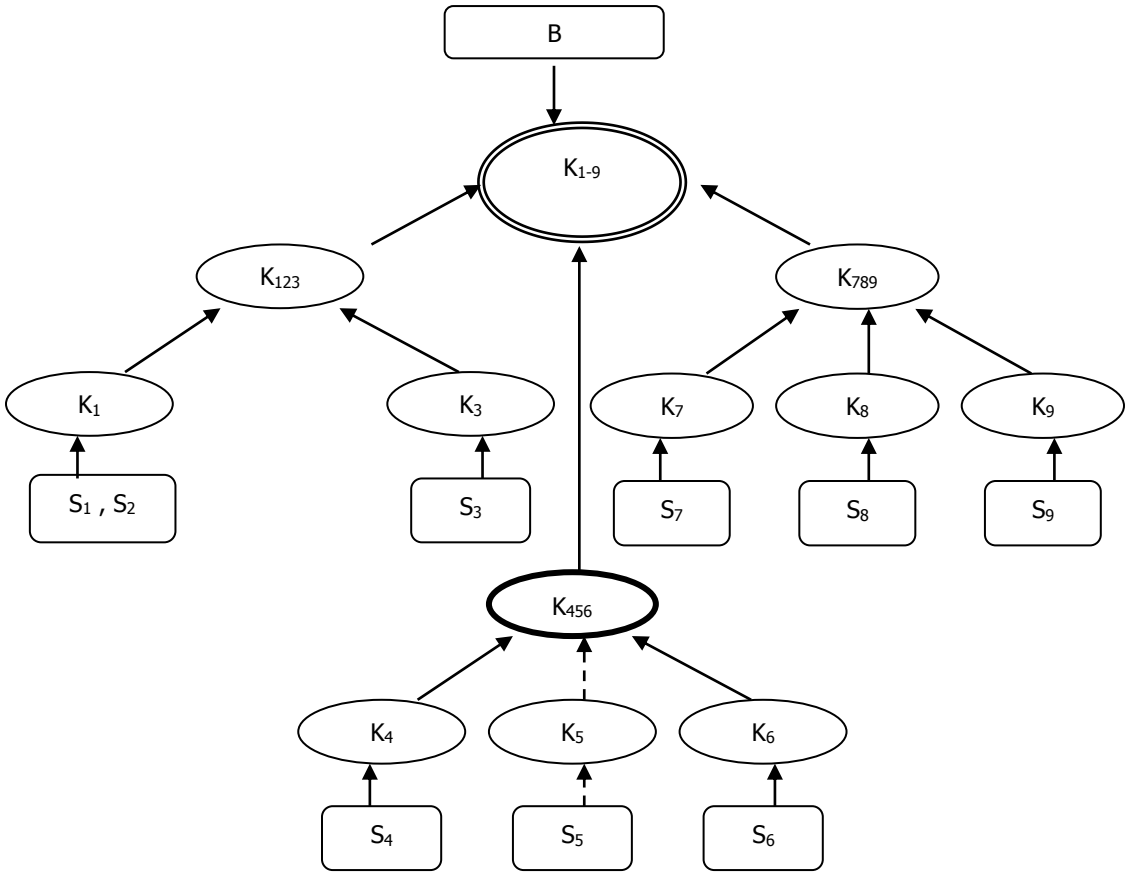


Fig. 1 : The distribution of symmetric keys for SGC

The broadcaster (B) is responsible for group access control and key management. In particular, B securely distributes keys to the group of the recipients and maintains the user-key relation. Let us consider the case of the recipient S_5. When it joins the group, B distributes K_5, K_{456} and $K_{1\text{-}9}$ to S_5.

Join protocol:

$S_j \rightarrow$ B: request for join
B : authenticate S_j and distribute individual key k_j
B: randomly generate a new group key k_g and a set of sub-group keys (k_{sg})
B $\rightarrow S_j$: $\{k_g , k_{sg}\}k_j$ /* k_g and k_{sg} are encrypted with the key k_j */

Change of subgroup: Suppose, S_5 departs from the old sub group sg_2 and wants to join a new subgroup sg_3.

B should replace the subgroup keys K_{456} and K_{789} with K_{46} and K_{5789} respectively. Thus, S_5 can not access any future communication of the subgroup sg_2. Also, S_5 cannot access any past communication of the subgroup sg_3. The rekeying process has been shown in figure 2.

Protocol for change of subgroup **:**

$S_j \rightarrow$ B : {request for leaving the old subgroup *sg*; request for joining a new subgroup sg'}k_j
B $\rightarrow S_j$: {leave-granted}k_j
B : Delete the old subgroup key k_{sg} if old subgroup is empty or randomly generate a new sub-group

key k'_{sg} for the subgroup *sg* to replace k_{sg} if old subgroup isn't empty.
randomly generate a new sub-group key $k'_{sg'}$ for the subgroup *sg'* to replace $k_{sg'}$
for each recipient S_i of the subgroup *sg* except the leaving member S_j do
$B \rightarrow S_i$: $\{k'_{sg}\}k_i$
for each supplier S_m of the subgroup *sg'* including S_j do
$B \rightarrow S_m$: $\{k'_{sg'}\}k_m$

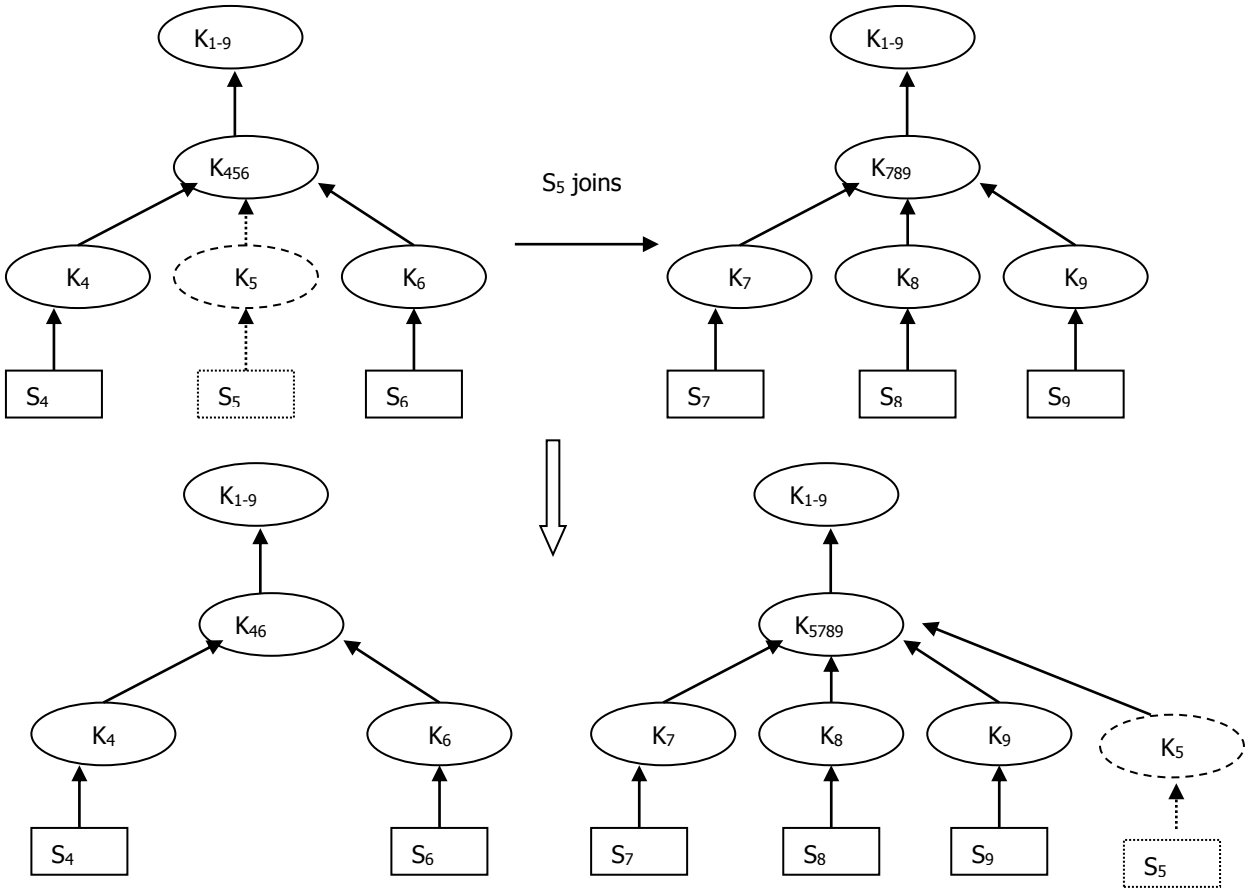


Fig. 2 : Key management for change of subgroup

Leave : If S_5 wants to regret and departs from the group (S_1 –S_9), the keys K_{456} and $K_{1\text{-}9}$ should be replaced with keys K_{46} and $K'_{1\text{-}9}$ respectively. Now, B encrypts $K'_{1\text{-}9}$ with K_{123}, K_{46} and K_{789} separately; encrypts K_{46} with K_4 and K_6 separately and then multicasts these encrypted keys (figure 3).

Leave protocol

$B \rightarrow S_j$: {leave group}k_j
B : randomly generate a new group key k'_g for the members of the group *g* to replace k_g
randomly generate a new sub-group key k'_{sg} for the subgroup sg to replace k_{sg}
for each subgroup sg' in the group g except the subgroup *sg* do
$B \rightarrow \{S\}_{sg'}$: $\{k'_g\}k_{sg'}$
for each supplier S_i of the subgroup *sg* except the leaving member S_j do
$B \rightarrow S_i$: $\{k'_g , k'_{sg}\}k_i$

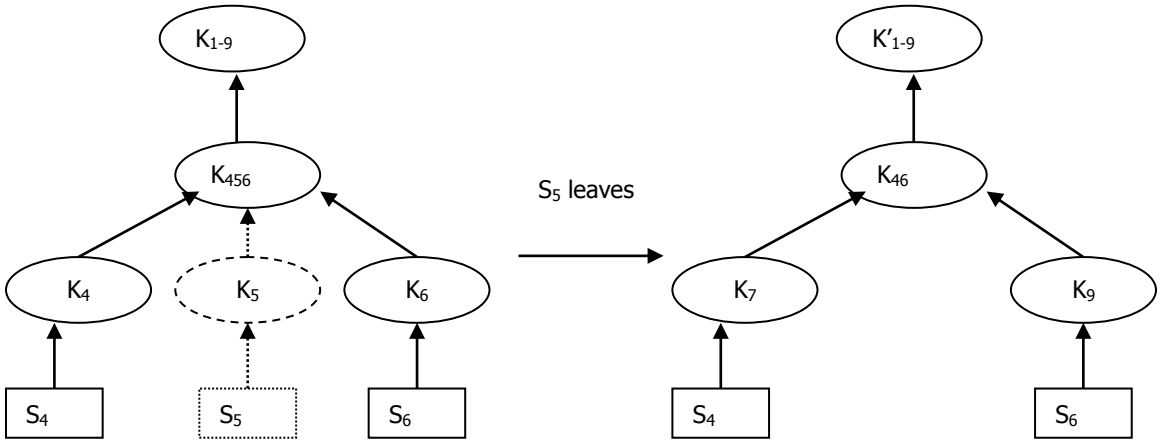


Fig. 3 : Key management for leave from the group

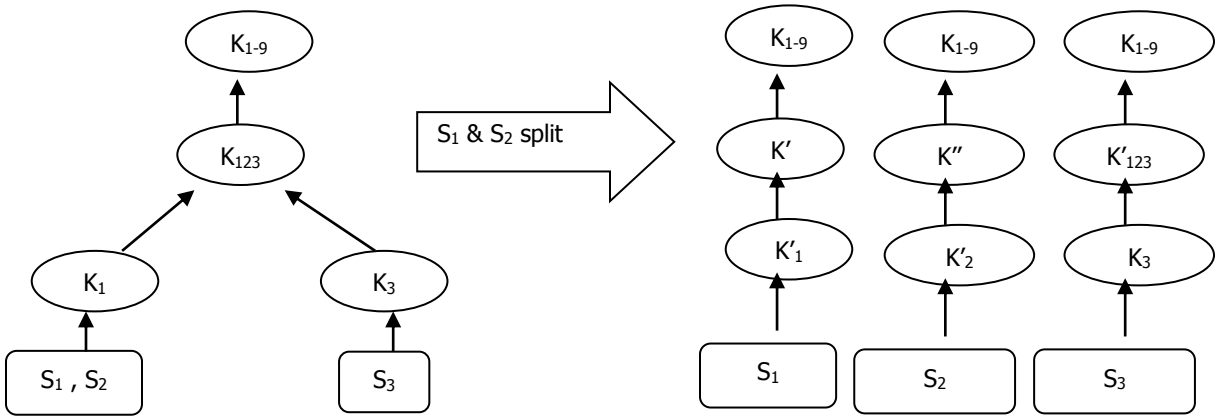
Split : Two or more recipients my split. So, S_1 and S_2 have decided to get splitted and form two or more new subgroups - sg_1' and sg_1''. Now, the key management strategy of B should be as follows to ensure forward and backward privacy :

(a) B should generate new subgroup keys K' and K" for the new splitted subgroups sg_1' and sg_1''. B should also generate new individual keys K_1' and K_2' for S_1 and S_2 respectively and delete old individual key K_1.

(b) If the splitted subgroups already exist, B should replace the old subgroup keys with new subgroup keys. This ensures backward privacy. Here, sg_1' and sg_1'' are two new subgroups. So, there is no requirement of replacement of old subgroup keys.

(c) B should replace old subgroup key of the merged subgroup if the subgroup is not empty. It ensures forward privacy. Since, S_3 remains the member of the subgroup sg_1 after the split of S_1 and S_2; so the old subgroup key K_{123} should be replaced with K'_{123}.

(d) B should delete the old subgroup key of merged subgroup if the subgroup is empty after the split. The subgroup sg_1 is not empty after the split of S_1 and S_2, so there is no requirement of the deletion of old subgroup key K_{123}.



S_1& S_2, S_3 bids for i_1,i_2

S_1, S_2, S_3 bid for i_1,i_2 and (i_1,i_2) respectively

Fig. 4 : Key management for split

***Protocol for split*:**

$S_j \rightarrow$ B: {request for split into two or more subgroups}k_j

B : Generate new subgroup keys and individual keys for the new splitted subgroups;

ELSE if the splitted subgroups already exist, replace the old subgroup keys with new subgroup keys ;

Delete the individual key of the merged recipients after the split;

Delete the old subgroup key of merged subgroup if the subgroup is empty after the split;

ELSE replace old subgroup key of the merged subgroup if the subgroup is not empty.

Merge : Two or more recipients may merge and form a sub-group to satisfy the demand of the broadcaster. For example, S_3 and S_9 have decided to merge. Now, the key management strategy of B should be as follows to ensure forward and backward privacy:

(a) B should generate new subgroup key for the merged subgroup if it is a new subgroup. In our example, sg_2 is not a new subgroup. It already exists. But, the individual keys of S_3 and S_9 should be replaced by a common individual key K_{39}

(b) B should replace old subgroup key of the merged sub-group if the sub-group already exists. Here, the old sub-group key of sg_2 i.e. K_{456} should be replaced by a new sub-group key K_{34569}. It ensures backward privacy since S_3 and S_9 will not be able to access past communications of the subgroup sg_2.

(c) B should delete old subgroup keys if the subgroups are empty after the merger. This is not applicable for our example since after merger, S_1 and S_2 belongs to sg_1 and S_7 and S_8 belongs to sg_3

(d) B should replace old subgroup keys if the subgroups are not empty after the merger. In other words, the subgroup key of sg_1 and sg_3 i.e. K_{123} and K_{789} should be replaced by K_{12} and K_{78} respectively. The new key-tree is shown in figure 5.

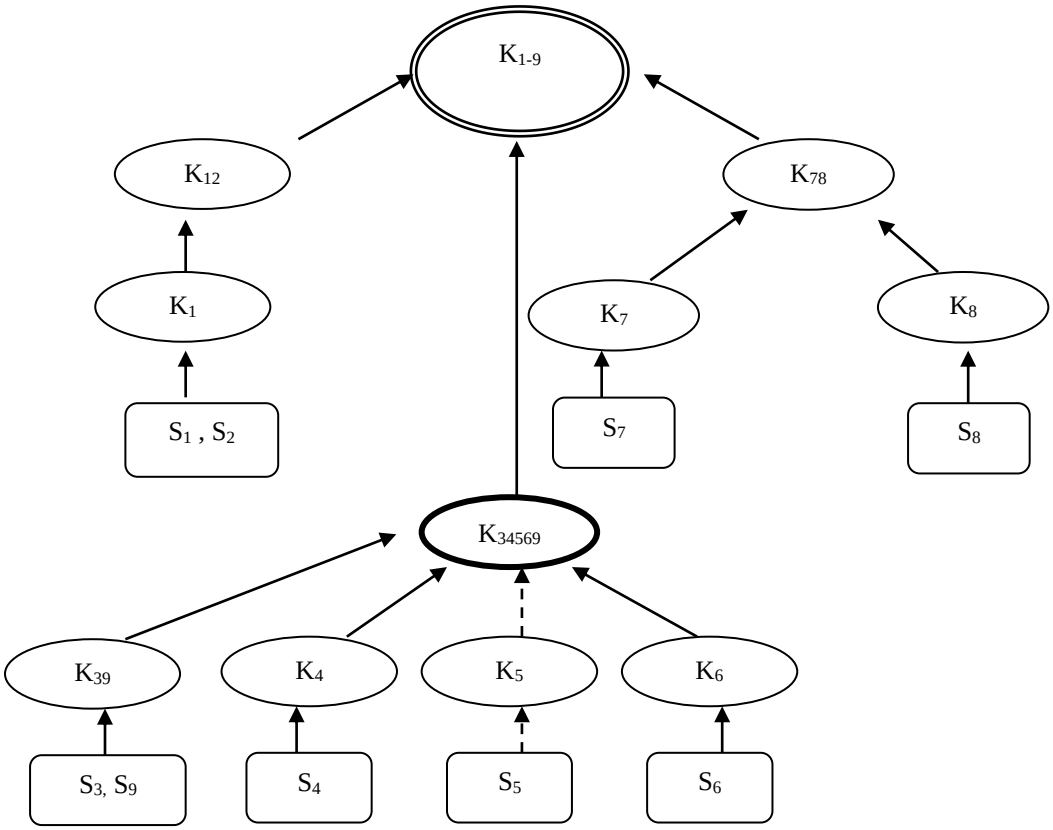


Fig. 5 : Key management for merger

***Protocol for merge*:**

$S_j \rightarrow$ B : {request for merger with one or more recipients to form a subgroup sg''}k_j

B : Generate new individual key of the merged recipients and delete their old individual keys.
Generate new subgroup key for sg" if sg" is a new subgroup;
ELSE replace old subgroup key of sg" if sg"already exists;
Replace old subgroup keys if the subgroups are not empty after the merger;
ELSE delete old subgroup keys if the subgroups are empty after the merger;

4. SYSTEM ARCHITECTURE

Security Intelligence			
Exploratory module : locate errors	**Fault finding: Cause-effect analysis**	**Diagnostics tool: program model checking**	**Real-time system verification**
Threat analytics		**Model checking algorithms**	
Automated verification		**Semi-automated verification**	
Communication protocol	**Broadcast schedule**	**Payment function**	
Adaptively Secure Broadcast Mechanism (ASBM)			

Figure 1 : Automated Verification System Architecture

This section outlines the architecture of an adaptively secure broadcasting system based on the proposed mechanism (ASBM). The architecture outlines the basic overview of application, computing, networking, data and security schema.

Application schema*:* The verification system must check three critical components of ASBM: communication protocol, broadcast schedule and payment function. It requires both automated and semi-automated verification options. The verification system calls threat analytics and a set of model checking algorithms for various phases : exploratory phase for locating errors, fault finding phase through cause effect analysis, diagnostics tool for program model checking and real-time system verification. Model checking is basically the process of automated verification of the properties of broadcasting communication system. Given a formal model of a system and property specification in some form of computational logic, the task is to validate whether or not the specification is satisfied in the model. If not, the model checker returns a counter example for the system's flawed behavior to support the debugging of the system. Another important aspect is to check whether or not a knowledge based system is consistent or contains anomalies through a set of diagnostics tools.

There are two different phases : explanatory phase to locate errors and fault finding phase to look for short error trails. Model checking is an efficient verification technique for communication protocol validation, embedded system, software programmes, workflow analysis and schedule check. The basic objective of the model checking algorithm is to locate errors in a system efficiently. If an error is found, the model checker produces a counter example how the errors occur for debugging of the system. A counter example may be the execution of the system i.e. a path or tree. A model checker is expected to find out error states efficiently and produce a simple counterexample. There are two primary approaches of model checking: symbolic and explicit state. Symbolic model checking applies a symbolic representation of the state set (e.g. BDD) for property validation. Explicit state approach searches the global state of a system by a transition function. Model checking algorithms often use heuristic search techniques such as A* and Depth First Search (DFS) algorithms. Its efficiency is measured in terms of automation and error reporting capabilities.

The broadcasting system must have a set of modules such as (b) threat analytics, (c) model checking, (d) data visualization and (e) system performance scorecard (SPS). These modules should be integrated with the core broadcast communication system through efficient interfaces. The application should have

following components: file, components, history, tools and help. The components module should have anti-virus, anti-spyware, e-mail scanner; update manager, license, system protection analyzer and identity protection sub-modules. The history module should have scan results, virus vault and event history log submodules. The tools should have scan computer, scan selected folder, scan file, update and advanced settings. The speed and priority of scanning should be controlled through user interface. The scan results should show the entities, tested objects, scan results, infections, spyware, warnings and root kits. The virus vault should have event history, virus name, path to file and original object name.

***Security schema**:* The verification system should analyze the security intelligence of the broadcasting system based on collective intelligence comprehensively. The output of the verification system is expected to be security intelligence in terms of authentication, authorization, correct identification, privacy: group, forward and backward, audit; fairness, correctness, transparency, accountability, confidentiality, trust, integrity, non-repudiation, commitment, reliability, consistency; liveness, deadlock freeness, lack of synchronization, safety and reachability. The security intelligence should be verified by threat analytics. It should assesses and mitigate the risks of false data injection, sybil, node replication, wormhole, blackhole, jellyfish, rushing, neighbor, coremelt, node deletion, flaws in broadcast schedule, poor QoS, malicious business intelligence, corruption in secret sharing, information leakage and shilling attack on the broadcasting system. The threat analytics should analyze system performance, sensitivity, trends, exception and alerts along two dimensions – time and insights. The analysis on time dimension may be as follows: what is corrupted or compromised in the broadcasting system: agents, communication schema, data schema, application schema, computing schema and broadcast mechanism? what occurred? what is occuring? what will occur? Assess probability of occurrence and impact. The analysis on insights may be as follows : how and why did the threat occur? What is the output of cause-effect analysis? The analytics also recommends what is the next best action? It predicts what is the best or worst that can happen?

***Computing schema**:* The computing schema is mainly associated with threat analytics and model checking algorithms. They interact with each other in real-time in an web enabled distributed computing environment. The threat analytics should be equipped with a set of data visualization tools and system performance scorecard.

***Data schema**:* The data structure should have specific data of various entities such as service provider or broadcaster, service consumers or receiving agents, broadcasting services: channels, packages, payment functions and contractual terms. The data schema of threat analytics

***Networking schema**:* It should have a wireless internet schema in distributed computing environment.

5. CONCLUSION

ASBM is applicable to the design and analysis of intelligent mechanisms in combinatorial auction or reverse auction for e-market, digital advertising, financial service (e.g. stock and derivatives), cloud computing, digital content distribution (e.g. software, e-films, e-music, e-books, e-publishing), e-governance, e-healthcare, radio and TV broadcast, SCADA and sensor networks. The concept is applicable to the design of efficient 1-n-p negation protocol for combinatorial reverse auction in supply chain management [14]. The basic objective of ASBM is to verify the security intelligence of a broadcasting system. This study can be extended in various ways.

A broadcasting system is expected to be a resilient system. The resiliency measures the ability to and the speed at which the system can return to normal performance level following a disruption. Real-time security management involves high cost of computation and communication. The vulnerability of the system to a disruptive event should be viewed as a combination of likelihood of a disruption and its potential severity. The system administrator must do two critical tasks: assess risks and mitigate the assessed risks. To assess risks, the system administrator should explore basic security intelligence: what can go wrong in broadcast operation? what is the probability of the disruption? how severe it will be? what are the consequences if the disruption occurs? A vulnerability map can be modeled through a set of expected risk metrics, probability of disruptive event and the magnitude of consequences. For example, the map has four quadrants in a two dimensional space; the vertical axis represents the probability of disruptive event and the horizontal axis represents the magnitude of the consequences.

The system administrator may face a set of challenges to solve the problem of resiliency: what are the critical issues to be focused on? what can be done to reduce the probability of a disruption? what can be done to reduce the impact of a disruption? How to improve the resiliency of the broadcasting system? The critical steps of risk assessment are to identify a set of feasible risk metrics; assess the probability of each risk metric; assess severity of each risk metric and plot each risk metric in the vulnerability map. The critical steps of risk mitigation are to prioritize risks; do causal analysis for each risk metric; develop specific strategies for each cell of vulnerability map and be adaptive and do real-time system monitoring.
A test bed can be modeled using firewalls and digital simulator for simulating field devices and RTUs. The test bed can be used for simulation of security protocols, identification or detection, classification and prioritization of various types of threats and vulnerabilities, practical implementation of verification mechanisms and computational and communication complexity analysis. Using simulation, it is possible to study how the number of attackers and their strategic moves affect the performance of a multicast session in terms of packet delivery ratio, throughput and end-to-end delay, and delay jitter. The experimental simulation results can show how a broadcasting system performs and behaves under various attack scenarios and the impact of counter attack measures.
Innovative broadcasting systems should be designed based on smart service oriented computing, networking, data, application and security schema. It is an interesting research agenda to explore intelligent strategic moves for model checking and communication protocol of a broadcasting system. The list as stated in this work may not be an exhaustive one. One of the limitations of ASBM is that it has not considered miscellaneous technical snags that may occur in a broadcasting system due to various reasons such as failure of electrical and electronic support, satellite communication link failure, supply chain disruption in rural and remote zones, natural disaster and computer virus attack. The knowledge should be extracted by interviewing network security experts and broadcast system administrators. Another critical agenda is to improve the cost of computation and communication in private broadcast. The business intelligence of the broadcasting mechanism may be explored through innovative payment function, penalty function and pricing algorithms based on algorithmic game theory and secure multi-party computation.

REFERENCES

1. A.Perrig, R. Canetti, D. Song and J.D. Tygar, Efficient and secure source authentication for multicast. NDSS'2001, 35-46.
2. A. Perrig, R. Canetti, J.D. Tygar, and D. Song. The TESLA broadcast authentication protocol. *RSA CryptoBytes,* 5(Summer), 2002.
3. A.Perrig The BiBa one-time signature and broadcast authentication protocol. In *Proceedings of the 8th ACM Conference on Computer and Communications Security,* pages 2S-37. ACM Press, November 2001.
4. M.Hirt and V.Zikas. Adaptively secure Broadcast, Eurocrypt'2010, LNCS 6110, 466 - 485, 2010.
5. J.A. Garay, J.Katz, R.Kumarasen and H.Zhou. Adaptively secure broadcast revisited.
6. R. Canetti, J. A. Garay, G. Itkis, D. Micciancio, M. Naor and B. Pinkas. Multicast security: taxonomy and some efficient constructions. In INFOCOM, 708 -716, 1999.
7. C.K.Wong, M.Gouda and S.S.Lam. 1998. Secure group communications using key graphs. ACM SIGCOMM Computer Communication Review, vol. 28, no. 4.
8. S. Rafaeli and D. Hutchison, A survey of key management for secure group communication, ACM Computing Surveys, 35(3), 309 - 329, 2003.
9. A. Clemanti, A. Monti, F.Pasquale and R. Silvestri. 2009. Broadcasting in dynamic radio networks. Journal of Computer and System Sciences, 75(4), 213-230.
10. S. Panjwani. Tackling adaptive corruptions in multicast encryption protocols. In S. P. Vadhan, editor, TCC, LNCS 4392, 21- 40. Springer, 2007.
11. L. Lamport, R. Shostak, and M. Pease. The Byzantine generals problem. ACM Transactions on Programming Languages and Systems, 4(3):382 - 401, 1982.
12. G.Kol and M.Naor. Cryptography and game theory: Designing protocols for exchanging Information. Proceedings from 5th Theory of Cryptography Conference (TCC), 2008.

13. S.Chakraborty. A study of several privacy-preserving multi-party negotiation problems with applications to supply chain management. Doctoral dissertation (unpublished), Indian Institute of Management Calcutta, 2007.
14. S.Chakraborty, S.K.Sharma and A.K. Pal. Privacy-preserving 1-n-p negotiation protocol, Hawaii International Conference on System Sciences (HICSS-41), Hawaii, USA, 2008.
15. B.Kalyansundaram, K.Pruhs and M. Velauthapillai. 2000. Scheduling broadcasts in wireless networks. In European Symposium of Algorithms, LNCS1879, Springer Verlag, 290-301.
16. J.Kim and K.Chahwa. 2004. Scheduling broadcasts with deadlines. Theoretical Computer Science, volume 325(3): 479-488.
17. A. Fiat and M. Naor. Broadcast encryption. In Douglas R. Stinson, editor, CRYPTO, LNCS 773, 480 - 491, Springer, 1993.
18. R. Merkle. A certified digital signature. In *Advances in Cryptology - CRYPTO* '89, volume 435, LNCS, 218- 238. Springer-Verlag, Berlin Germany, 1990.
19. W.Mao, Modern Cryptography Theory & Practice, Pearson Education,2007.
20. Y.Zheng. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption). LNCS 1318, Springer-Verlag.
21. Berard, B., Bidoit,M., Finkel,A., Laroussinite, F., Petit, A., Petrucci, L., Schnoebelen, Ph. and Mckenzie,P. 2001. Systems and software verification. Springer.
22. S. Chakraborty, Digital defense : Verification of security intelligence. Technical report. 2012.
23. M.Gertz and S.Jajodia. 2008. Handbook of database security applications and trends.
24. Y. Oren and A.D. Keromytis. 2014. From the Aether to the Ethernet - Attacking the Internet using Broadcast Digital Television. 23rd USENIX Security Symposium. August 20-22, USA.
25. A. Shamir. How to share a secret. Communications of the ACM, volume 22, 612 - 613,1979.
26. R. Merkle. Secure communication over insecure channels. *Communications of the ACM,* 21(4):294-299, April 1978.
27. M.Shema. edited by A.Ely. 2010. Seven deadliest web application attacks. Elsevier.
28. A.Studer and A.Perrig. 2008. The Coremelt attack.
29. J.Douceur. 2002. The sybil attack. Proceedings of Workshop on P2P systems (IPTPS).
30. Pal,A.K., Nath,D. and Chakraborty,S. 2010. A Discriminatory Rewarding Mechanism for Sybil Detection with Applications to Tor, WASET.
31. A.Seshadri, A.Perrig, L.van Doorn and P.Khosla.2004. SWATT: Software based attestation for embedded devices. Proceedings of IEEE Symposium on Security and Privacy, Oakland, California.
32. S. Berkovits. How to broadcast a secret. In Advances in Cryptology - Eurocrypt'91, volume 547, LNCS 535-54l. Springer-Verlag, Berlin Germany, 1991.