SECURITY INTELLIGENCE FOR BROADCAST: THREAT ANALYTICS

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

Abstract: This work presents an Adaptively Secure Broadcast Mechanism (ASBM) based on threats analytics and case based reasoning. 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, computational intelligence and business intelligence. 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 a 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.

Keywords: Broadcast Mechanism, Security intelligence, Computational intelligence, Communication complexity, Business intelligence

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?

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 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, SMC 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 and business intelligence. Section 4 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.

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}

   s.t. ***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: do *commitment* 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* ppdm (randomization, summarization, aggregation, generalization, suppression, de-identification, 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* broadcasts 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*** :

4.1 call threat analytics and assess risks of single or multiple attacks on broadcasting system : {false data injection attack, 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, shilling attack};

4.2 do verification of security intelligence : {authentication, authorization, correct identification, privacy: group, forward and backward, audit, fairness, correctness, transparency, trust, reliability and accountability};

if < detect false data injection attack > then < R checks fairness, correctness of broadcast; alerts S and A; identify the sources of data corruption>;

else if < S is compromised > *then* < R alerts A else A alerts R; do verification of correct identity and authenticity of S; validate access control policy>;

else if < A is compromised > *then* < R complains to A at first. If A is inactive, the recipients adopt tit-for-tat strategy and complains to the regulator at higher level of authorization, give threats, reject broadcast or change service provider >;

else if < R is compromised > then < R_i alerts S and A to verify corruption in secret sharing. S *or* A checks group, forward and backward privacy by verifying access control policy during join, leave, merge, split and subgroup change of the recipients >;

else if < the communication channel is compromised > *then* < verify the risk of wormhole attack; check flaws in web security; S alerts R, A *or* R alerts S, A *or* A alerts S, R >;

else if < detect coremelt *or* blackhole *or* jellyfish *or* rushing *or* neighbor attack > *then* < R alerts S; S alerts A; do traffic congestion analysis >;

else if < sense sybil or node replication or node deletion attack > *then* < call tracing mechanism : verify e-passport or trusted explicit and implicit certification of nodes; do resource testing; call challenge response protocol for sensor node attestation verification >;

else if < sense flaws in broadcast schedule > *then* < R alerts S and A : verify commitment in negotiated plan, delay in schedule *or* error in scheduling logic *or* exception handling error or replay attack >;

else if < sense poor QoS > *then* < verify denial of service *or* non-repudiation *or* network connectivity and internet speed *or* data corruption *or* noisy signal *or* data loss *or* data integrity *or* call drop *or* disruption in energy supply; R alerts S and A to resolve technical snags >;

else if < sense malicious business intelligence > *then* < 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 >;

else if < sense shilling attack > *then* < do performance analysis: ad slot allocation, content of adwords: fraudulent recommendation, exposure time and frequency, customization, delivery, click rate, impression >;

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

Output: P_b, Security intelligence.

3. COMPLEXITY ANALYSIS OF ASBM

3.1 Communication Complexity

Theorem 1: 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. There is scope of secure multi-party computation based on broadcasted data.

3.2 Computational Intelligence

Theorem 2 : The cost of computation of ASBM is a function of the complexity and efficiency of security algorithms.

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.

Theorem 3: 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]. 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]. 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.

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.

3.3 Security Intelligence

Model checking is an automated technique for verifying a finite state concurrent system. Model checking has three steps: represent a system by automata, represent the property of a system by logic and design model checking algorithm. Model checking verifies specific set of properties of a system such as reachability, safety, liveness, deadlock freeness and fairness [21]. 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.

Theorem 4: The security intelligence of ASBM is explored through threat analytics.

ASBA defines security intelligence in terms of authentication, authorization, correct identification, privacy: group, forward and backward, audit, fairness, correctness, transparency, trust, reliability and accountability of the broadcasting system. The algorithm 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. The basic objective of digital defense is to verify the security intelligence of a broadcasting system and to protect the system from a set of threats and malicious attacks.

Theorem 5: **ASBM explores different scenarios of corruption in terms of broadcasting agent, system administrator, recipients, communication channel and broadcast data. It verifies security intelligence through efficient tracing and revocation mechanism.**

In ASBM, corruption may occur in various ways [25]. 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 all the agents (S, A and R), communication channel and broadcast data are free of corruption.

Theorem 6: A corrupted communication channel is a real threat to a web enabled broadcasting system; another threat is wormhole 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 [26,27].

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 7: The recipients must verify the fairness, trust and correctness of broadcast data to detect false data injection attack and mitigate the risk through social choice.

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. 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 music, films, dramas and reality shows. Old telecasts are often broadcasted as live telecasts through replay attack. 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 and secure multi-party computation. 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.

Theorem 8: The broadcasting system should monitor traffic congestion and QoS in real time to avoid coremelt, blackhole, jellyfish, neighbor and rushing 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.

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 of 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 9: Efficient and intelligent tracing mechanisms are essential to detect sybil, node replication and node deletion 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.

/* *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 & 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. */

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.

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.

3.4 Business Intelligence

Theorem 10: **The business intelligence of ASBM depends on payment function and quality of broadcasted data stream.**

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.

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 secure multi-party computation jointly.

4. 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. For example, 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. An important research agenda is to improve the resiliency of a broadcasting system against various types of malicious attacks using analytics. The broadcasting system is expected to be a resilient system. A vulnerability map can be modeled through a set of expected risk metrics, probability of disruptive event and the magnitude of consequences. Different types of experiments may be conducted on a broadcasting system through simulation of various malicious attacks. 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 existing list 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.