ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Security-Sensitive Applications using TAM: in Multicast Protocol

R. Srikkanthan A.P and Dr. V. Khana

Dean, Bharath University

ARTICLE INFO

Article history:
Received 28 January 2015
Accepted 25 February 2015
Available online 6 March 2015

Keywords:
TAM, Ad-Hoc Networks,multicast.

ABSTRACT

This paper has presented TAM, which pursues a two tired hierarchical strategy combining both time and secret-information asymmetry in order to achieve scalability and resource efficiency. The performance of TAM has been analyzed mathematically and through simulation, confirming its effectiveness. The simulation and analytical results demonstrate the performance advantage of TAM in terms of bandwidth overhead and delivery delay. A new Tiered Authentication scheme for Multicast traffic (TAM) for large scale dense ad-hoc networks. TAM combines the advantages of the time asymmetry and the secret information asymmetry paradigms and exploits network clustering to reduce overhead and ensure scalability. Multicast traffic within a cluster employs a one-way hash function chain in order to authenticate the message source.

To Cite This Article: R. Srikkanthan A.P and Dr. V. Khana, Security-Sensitive Applications using TAM: in Multicast Protocol. ***Aust. J. Basic & Appl. Sci.,*** *9(10): 69-73, 2015*

INTRODUCTION

The continual advancement in wireless technologies has enabled networked-solutions for many nonconventional civil and military applications. In recent years ad-hoc networks have been attracting increased attention from the research and engineering community, motivated by applications like digital battlefield, asset tracking, air-borne safety, situational awareness, and border protection. In these network applications, it is important to devise efficient network management solutions suitable for nodes that are constrained in onboard energy and in their computation and communication capacities. In addition, the solutions must be scalable to support networks covering vast areas with a large set of nodes that communicate over many hops. These characteristics make the design and management of ad-hoc networks significantly challenging in comparison to contemporary networks.

Group communication is considered a critical service in adhoc networks due to their inherently collaborative operations, where the nodes cooperate in network management and strive to accomplish common missions autonomously in highly unpredictable environment without reliance on infrastructure equipment. For example, in combat missions troops report their status and share observed data in order to become aware of the overall situation and coordinate their actions. In addition, it is common for ad-hoc networks to rely on multicast for management-related control traffic such as neighbor/route discovery to setup multi-hop paths, the establishment of time synchronization, etc. Such multicast traffic among the nodes has to be delivered in a secure and trusted manner. In particular the provided network services need to achieve the following security goals: (1) Confidentiality, to prevent adversaries from reading transmitted data, (2) Message integrity, to prevent tampering with transmitted messages, and (3) Source Authentication, to prevent man-in-the-middle attacks that may replay transmitted data for node impersonation. Confidentiality is achieved by encrypting the transmitted data. The work presented in this paper aims at addressing the second and third goals. Providing an efficient multicast message and source authentication security service that can easily scale for large networks is an important capability for the operation and management of the underlying network.

Related works:

H. Yang et.al proposes (Yang, 2004), Due to the dynamic nature of WAHN communications and the multi-node involvement in most WAHN applications, group key management has been proposed for efficient support of secure communications in WAHNs. Exclusion Basis Systems (EBS) provide a framework for scalable and efficient group key management where the number of keys per node and the number of re-key messages can be relatively adjusted. EBS-based solutions,

Corresponding Author: R. Srikkanthan, Dean, Bharath University
E-mail: srikkanthan.r@gmail.com

however, may suffer from collusion attacks, where a number of nodes may collaborate to reveal all system keys and consequently capture the network. In this paper we investigate the collusion problem in EBS anddemonstrate that a careful assignment of keys to nodes reduces collusion. Since an optimal assignment is NP hard, we propose a location-based heuristic where keys are assigned to neighboring nodes depending on the hamming distance between the strings of bits representing the used subset of the keys employed in the system. Simulation results have demonstrated that our proposed solution significantly boosts the network resilience to potential collusion threats.

Perrig et.al Proposes (Perrig, 2000), One of the main challenges of securing multicast communication is source authentication, or enabling receivers of multicast data to verify that the received data originated with the claimed source and was not modified enroute. The problem becomes more complex in common settings where other receivers of the data are not trusted, and where lost packets are not retransmitted. Several source authentication schemes for multicast have been suggested in the past, but none of these schemes is satisfactorily efficient in all prominent parameters. We recently proposed a very efficient scheme, TESLA that is based on initial loose time synchronization between the sender and the receivers, followed by delayed release of keys by the sender. This paper proposes several substantial modifications and improvements to TESLA. One modification allows receivers to authenticate most packets as soon as they arrive (whereas TESLA requires buffering packets at the receiver side, and provides delayed authentication only). Other modifications improve the scalability of the scheme, reduce the space overhead for multiple instances, increase its resistance to denial-of-service attacks, and more.

R. Canetti et al., propose a human-based model which builds a trust relationship between nodes in an ad hoc network. The trust is based on previous individual experiences and on the recommendations of others. We present the Recommendation Exchange Protocol (REP) which allows nodes to exchange recommendations about their neighbors. Our proposal does not require disseminating the trust information over the entire network. Instead, nodes only need to keep and exchange trust information about nodes within the radio range. Without the need for a global trust knowledge, our proposal scales well for large networks while still reducing the number of exchanged messages and therefore the energy consumption. In addition, we mitigate the effect of colluding attacks composed of liars in the network. A key concept we introduce is the relationship maturity, which allows nodes to improve the efficiency of the proposed model for mobile scenarios. We show the correctness of our model in a single-hop network through simulations. We also extend the analysis to mobile multihop networks, showing the benefits of the maturity relationship concept. We evaluate the impact of malicious nodes that send false recommendations to degrade the efficiency of the trust model. At last, we analyze the performance of the REP protocol and show its scalability. We show that our implementation of REP can significantly reduce the number messages.

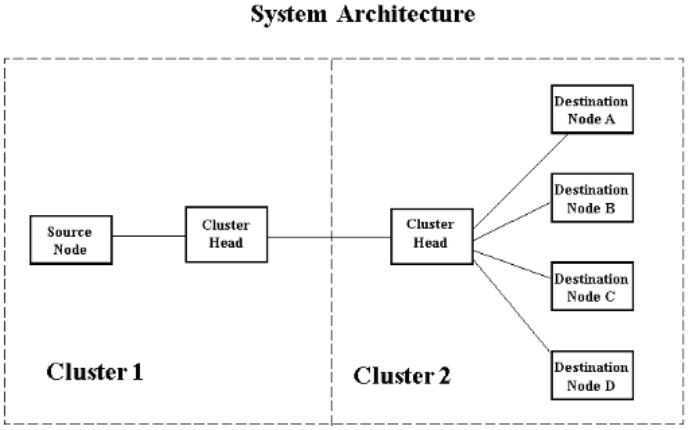

Fig. 1: Architecture Diagram.

Existing system:

EBS-based solutions, however, may suffer from collusion attacks, where a number of nodes may collaborate to reveal all system keys and consequently capture the network. In this paper we investigate the collusion problem in EBS and demonstrate that a careful assignment of keys to nodes reduces collusion. Since an optimal assignment is NP hard, we propose a location-based heuristic where keys are assigned to neighboring nodes depending on the hamming distance between the strings of bits representing the used subset of the keys employed in the system.

Source authentication schemes found in the literature can be classified into three categories: (1) secret information asymmetry, (2) time asymmetry,

and (3) hybrid asymmetry .The asymmetry property denotes that a receiver can verify the message origin using the MAC in a packet without knowing how to generate the MAC. This property is the key for preventing impersonation of data sources. In secret information asymmetry every node is assigned a share in a secret, e.g., a set of keys. A source appends MACs for the multicast keys so that a receiver verifies the authenticity of the message without being able to forge the MACs for the other nodes. The challenge in using this category of approaches is striking the balance between collusion resilience and performance impact. While the use of a distinct MAC per node imposes prohibitive bandwidth overhead, relying on the uniqueness of the key combinations risks susceptibility to node collusion. TAM pursues secret information asymmetry for its inter-cluster operation and limits the key pool size to suit only the number of clusters. While the description of TAM in Section IV assumes the use of other schemes are equally applicable.

The main idea behind time asymmetry is to tie the validity of the MAC to a specific duration so that a forged packet can be discarded. One-way hash chains are usually employed to generate a series of keys so that a receiver can verify the current key based on an old key without being able to guess the future key. Initially, a source picks a key K0 and generates a chain of keys by recursively applying a one-way hashing function. These keys are used to form the MAC for the individual data packets. The source then reveals the last key, *Kl*, in the chain to all receivers to serve as the baseline for verification. The key which is used to generate the MAC of a packet is revealed after some time period so that the key cannot be used to impersonate the source.When revealed, the receiver validates the key using *Kl* or any of the previously revealed keys. TESLA is a very popular example of this category.

Proposed system:

These applications are characterized by the hostile environment that they serve in and by the multicast-style of communication traffic. Therefore, authenticating the source and ensuring the integrity of the message traffic become a fundamental requirement for the operation and management of the network. However, the limited computation and communication resources, the large scale deployment and the unguaranteed connectivity to trusted authorities make known solutions for wired and single-hop wireless networks inappropriate. This paper presents a new Tiered Authentication scheme for Multicast traffic (TAM) for large scale dense ad-hoc networks. TAM combines the advantages of the time asymmetry and the secret information asymmetry paradigms and exploits network clustering to reduce overhead and ensure scalability. Multicast traffic within a cluster employs a one-way hash function chain in order to authenticate the message source. Cross-cluster multicast traffic includes message authentication codes (MACs) that are based on a set of keys. Each cluster uses a unique subset of keys to look for its distinct combination of valid MACs in the message in order to authenticate the source. The simulation and analytical results demonstrate the performance advantage of TAM in terms of bandwidth overhead and delivery delay.

Tiered authentication of multicast:

TAM pursues a two-tier process for authenticating multicast traffic in ad-hoc networks. TAM uses clustering to partition a network, and then authenticates multicast traffic by employing time asymmetry for intra-cluster traffic and secret information asymmetry for inter-cluster traffic. As mentioned earlier, clustering is a popular scheme for supporting scalable network operation and management. Several studies have shown that the gains achieved by clustering supersede the overheard in forming and maintain the clusters TAM leverages such a network management scheme.

3.1 Intra-cluster Source Authentication:

Grouping nodes into clusters enables having a reasonably tight bound on the end-to-end delay of packet delivery and will thus enable the use of a time asymmetry based authentication scheme. Intra-cluster authentication in TAM is based on TESLA (Perrig, 2000). Inter-cluster multicast traffic will be authenticated differently as explained below. A source node generates a chain of onetime- use keys using the hash function, e.g., MD5, SHA-1, etc., and shares only that last generated key, *Kl*, with the receivers. A message can be authenticated only when the used key in the chain is revealed. To verify the authentication key, the receiver recursively applies the cryptographic hash function until reaching *Kl*. In reality, the receiver can stop when reaching a key that has been used before. A key cannot be used outside Its designated time interval and the message will be ignored if the MAC is based on an expired key. Consequently, clock synchronization is required to make sure that the source and destination have the same time reference for key expiration. Therefore, TAM favours small cluster diameters as will be shown shortly. The approach has two distinct advantages, namely:

The MAC overhead is small; basically a single MAC is used per every multicast packet for all receivers. A missed key in a lost packet would not obstruct the authentication process since a receiver can refer back to Kl. The size of the time interval, which determines when a key is revealed, depends on the clock jitter among nodes in the cluster and on the maximum end-to-end delay between a sender and receivers. Uncertainty about these factors causes the source to be extra conservative in revealing the keys and it thus slows down the data transmission rate. The size of the time interval, which determines when

a key is revealed, depends on the clock jitter among nodes in the cluster and on the maximum end-to-end delay between a sender and receivers. Uncertainty about these factors causes the source to be extra conservative in revealing the keys and it thus slows down the data transmission rate. Basically, the receiver will not be able to authenticate the packet contents until the key is transmitted in a later packet. The authentication delay may be unacceptable for the application. Perrig et al., (2000) have proposed the use of multiple chains in order to expedite the authentication process for close nodes without waiting until further nodes, that are reachable over congested paths, receive the packet. In TAM, the concern about the authentication delay is generally addressed by the fact that the cluster includes just a subset of the network nodes. The maximum end-to-end delay experienced by an intra cluster multicast will be mostly dependent on the cluster radius. By controlling the radius of the cluster at the time of cluster formation, i.e., deciding the distance in terms of the number of hops between a member node and the cluster-head (Canetti, 1999), it will be possible to tackle this issue. Furthermore, clustering will make it more feasible to synchronize the clock of the nodes in the cluster with some reasonable accuracy.

3.2 Inter-Cluster Authentication:

Authentication based on time asymmetry requires clock synchronization and thus does not suit large networks. For inter-cluster multicast traffic, TAM applies a strategy based on secret information asymmetry and engages the cluster-heads in the authentication process. Basically, the source "s" that belongs to Clusteri will send the multicast packets to the heads of all clusters that have designated receivers. For example, if the members of the multicast group for s are residing in clusters g, h, j, and k, node s sends the message to CHg, CHh, CHj, and CHk. These cluster heads will then forward the message to the receivers in their respective clusters. The rationale is that the MAC will be associated with the cluster rather than the nodes and thus the overhead is reduced significantly. In other words, the multicast from s consists of multiple multicasts; (1) from s to all relevant cluster heads, (2) a distinct multicast within each of the target clusters to relay the message to designated receivers. This can also be advantageous if node mobility is to be dealt with. A node that switches from one cluster to another would only introduce local changes and would not require special handling by the source with respect to the authentication process. The process goes as follows. The source will generate a pool of M keys. Each of the NCL clusters in the network will be assigned a share L of keys, with M < L× NCL. The key share will be sent securely, e.g. using asymmetric cryptographic protocol, to the heads of the individual clusters. The source will then append multiple MACs to the multicast packet; each MAC is based on a distinct key. For a broadcast, exactly M MACs will be included in a packet. The source "s" will then transmit the multicast message to the cluster-heads. Each CHj checks the MACs and confirm the source authenticity when a set of L MACs in the message are found to be based on the L keys assigned to CHj by s. The value of M and L is subject to trade-off between security and bandwidth overhead. For L = 1, M needs to be equal to NCL Higher values of *L* allow cutting the overhead by assigning unique key combinations to cluster heads (M = LogNCL), possibly at the expense of having a higher risk of collusions if multiple cluster-heads get captured by an adversary. The assignment of the key shares can be based on random selection of *L* keys from the key pool or based on a localized scheme that minimizes the probability of collusion (Ngai, 2006). It is worth mentioning that *NCL* would depend on the cluster radius and the used clustering algorithm. The performance of the single key per cluster versus the use of MAC combinations will be studied in Section VI using an analytical estimate of *NCL*. Fig. 3 illustrates how TAM handles inter-cluster multicast traffic. The multicast group of a source node "*s*" includes nodes "*a*1", "*b*1", "*z*1". First, node "*s*" prepares a MAC corresponding to every cluster targeted by the multicast and appends these MACs to the data packet. The source node then forwards the packet to *CHa*1, *CHb*1, *and CHz1*. Each of the receiving cluster-heads will authenticate the packet using their key share that they got from "s" at the time the multicast session was established. After authenticating the source, each cluster-head forwards the message to the members of the multicast group within its cluster. TAM intra-cluster authentication procedure will be followed inside each cluster, i.e., *CHa*1 will replace the inter-cluster MACs with an intra-cluster time asymmetry based MAC produced so that receivers like *a*1 can authenticate *CHa*1, and similarly for *CHb*1, . . . , *CHz*1. Again it is important to point out the high cost, in terms of bandwidth and power consumption, associated with signing every packet using asymmetric keys. That is why public/ private key pairs are used to establish initial trust. Even in unicast sessions the two peers never use asymmetric keys to sign traffic streams, they only use them once to pass a common shared secret, and then the unicast packets are signed using such shared secret. TAM uses asymmetric keys for cluster heads to establish trust with the source and get unique subset of authentication keys for the cluster.

Conclusion:

In recent years there has been a growing interest in the use of ad-hoc networks in security-sensitive applications such as digital battlefield, situation awareness, and border protection. The collaborative nature of these applications makes multicast traffic very common. Securing such traffic is of great importance, particularly authenticating the source

and message to prevent any infiltration attempts by an intruder. Contemporary source authentication schemes found in the literature either introduce excessive overhead or do not scale for large networks. This paper has presented TAM, which pursues a two tired hierarchical strategy combining both time and secret information asymmetry in order to achieve scalability and resource efficiency. The performance of TAM has been analyzed mathematically and through simulation, confirming its effectiveness. In addition, the effect of the various parameters has been studied and guidelines have been highlighted for picking the most suitable configuration in the context of the particular application requirements; most notably having a cluster radius of 2 or 3 hops appears to be the most suitable for TAM. Our future work plan includes studying the effect of different clustering strategies on the performance of TAM.

REFERENCES

Canetti, R., 1999. "Multicast security: a taxonomy and efficient constructions," in Proc. 1999 IEEE INFOCOM.

Ngai, E.C.H. and M.R. Lyu, 2006. "An authentication service based on trust and clustering in wireless ad hoc networks: description and security evaluation," in Proc. 2006 IEEE International Conf. Sensor Networks, Ubiquitous, Trustworthy Computing.

Perrig, A., R. Canetti, D. Song and D. Tygar, 2000. "Efficient authentication and signing of multicast streams over lossy channels," in Proc. 2000 IEEE Symposium Security Privacy.

Yang, H., 2004. "Security in mobile ad-hoc wireless networks: challenges and solutions," IEEE Wireless Commun. Mag., 11(1): 1536–1284.