Indian Journal of Emerging Electronics in Computer Communications-IJEECC, Vol.1, Issue.1,April 2014

Secure Authentication of Multicast protocol for Ad-Hoc Networks

D. Kanimozhi[*1], S. Divya Mary[*2], S.J. Gayathri Pillai[*3],
B. Devendar Rao[#4], M.L. Alphin Ezhil Manuel[#5]

[*1 ,*2,*3]*U.G Student, B.E CSE, Alpha College of Engg, Chennai, T.N, India.*
[#4.#5]*Assistant Professor, Dept of CSE, Alpha College of Engg, Chennai, T.N, India.*
kanimozhid3@gmail.com

Abstract—multicast stream authentication and signing is an important and challenging problem.applications such astroop coordination in a combat field, situational awareness, etc.the main challenges are fourfold.first,authenticity must be guaranteed even when only the sender of the data is trusted. Second, unguaranteed connectivity to trusted authorities make known solutions for wired and single hop wireless network inappropriate.we propose an efficient Scheme, 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.

Index Terms—Multicast communications, message authentication, ad-hoc networks.

I. 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. In addition, the great flexibility of ad-hoc networking comes at the price of an increased vulnerability to security attacks and trade-off would be unavoidable at the level of network management and services

A Challenges and Design Goals

Multiple factors make multicast authentication in ad-hoc networks very challenging. The issues are fundamentally due to the resource constraints and the wireless links. First, nodes have limited computing, bandwidth, and energy resources which make the overhead of basic asymmetric key-pair cryptography methods very expensive. In addition, the unstable wireless links due to radio interference cause frequent packet loss errors and require a security solution that can tolerate missed packets, as well as differentiate between packet retransmission and replay. Furthermore, the instability of the wireless links makes it unwise to rely on the continual involvement of a trusted authority in the generation and sharing of session keys since a stable connection cannot be guaranteed. On the other hand, while basic symmetric key cryptography methods are efficient, they are ineffective for multicast traffic patterns; since using a common key for all receivers will make it relatively easy to impersonate a sender by any of the receiving nodes.

B. Contribution and Organization

This paper proposes a new Tiered Authentication scheme for Multicast traffic (TAM) for ad-hoc networks. TAM exploits network clustering in order to cut overhead and ensure scalability. Multicast traffic within the same cluster employs one-way hash chains to authenticate the message source. The authentication code is appended to the message body. However, the authentication key is revealed after the message is delivered. The idea is similar to the Timed Efficient Stream Loss-tolerant authentication (TESLA) system. The relatively small-sized cluster would make it possible to keep the nodes synchronized and address the maximum variance in forwarding delay issue of message authentication within a cluster. On the other hand, cross-cluster multicast traffic includes message authentication codes (MACs) that are based on multiple keys. Each cluster looks for a distinct combination of MACs in the message in order to authenticate the source. The source generates the keys at the time of establishing the multicast session. The keys will be securely transmitted to the head of every cluster that hosts one or multiple receivers. The multicast message is then transmitted to the cluster-heads which authenticate the source and then deliver the message to the intended receivers using the intra-cluster authentication scheme. TAM thus combines the advantages of the secret information asymmetry and the time asymmetry paradigms. The analytical and numerical results demonstrate the performance advantage of TAM.

II . RELATED WORK

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.

III. SYSTEM MODEL

A Architectural Model

An ad-hoc network is a collection of autonomous node that together set up a topology without the support of a physical networking infrastructure. Depending on the applications, an ad-hoc network may include up to a few hundreds or even a thousand nodes. Communications among nodes are via multi-hop routes using Omni directional wireless broadcasts with limited transmission range.

Clustering is a popular architectural mechanism for enabling scalability of network management functions. It has been shown that clustered network topologies better support routing of multicast traffic and the performance gain dominates the overhead of creating and maintaining the cluster. Each cluster is controlled by a cluster head, which is reachable to all nodes in its cluster, either directly or over multi-hop paths. Fig. 1 shows an articulation of an example clustered network Nodes that have links to peers in other clusters would serve as gateways. The presence of gateways between two clusters implies that the heads of these clusters are reachable to each other over multi-hop path and that these two clusters are considered neighbors.

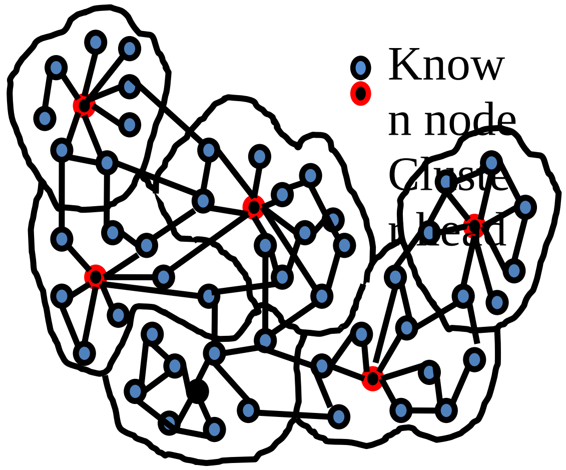

Fig 1. An example clustered ad-hoc network

If a node moves out its current cluster and joins another, it is assumed that the associated cluster-heads will conduct a handoff to update each other about the change in membership of their clusters; other cluster-heads will not be involved in the handoff events outside their clusters. Mobility is not the focus of this paper; however, prior studies have shown that clustering is advantageous for multicast routing in mobile environments.

IV. TIERED AUTHENTICATION OF MULTICAST TRAFFIC

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.

A 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 H' is the function for generating the MAC Fig. 2. A source used a key Ki during period j and reveals it in period j +1. thus, a packet in period j will have a MAC based on Ki and will also include Ki + 1 for authenticating the packet received in period j − 1. TESLA [4]. Inter-cluster multicast traffic will be authenticated differently as explained below. A source node generates a chain of one-time-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. Fig. 2 demonstrates the authentication process. 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 favors 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. Basically, the receiver will not be able to authenticate the packet contents until the key is transmitted in a later packet, as shown in Fig. 2. The authentication delay may be unacceptable for the application. Perrig et al., [4] 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.

A. 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 Cluster i 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.

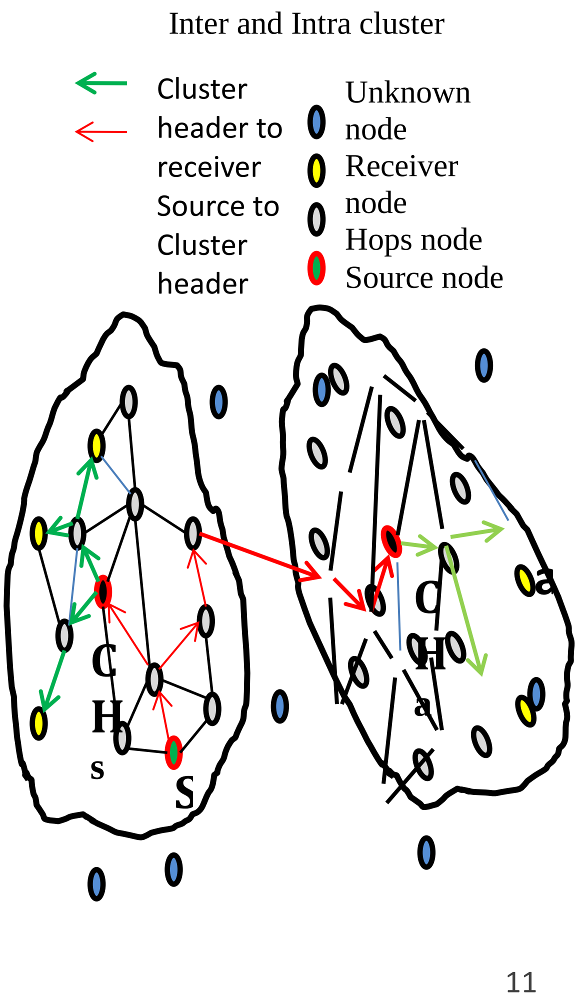

Fig.2. Summary of the TAM inter & intra-cluster operation

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.

V. PERFORMANCE ANALYSIS

The following analysis assumes a network of N nodes with a source is conducting a broadcast, i.e., sending a packet to all the other (N − 1) nodes. The focus is on the scalability property assessed based on the bandwidth and delay. The best and worst case performance are analyzed.

A. Baseline Performance

The baseline of comparison is a multicast over a flat network topology. As pointed out in Section II, time asymmetry can introduce vulnerability for large networks unless the data are generated at a very slow rate and excessive delivery delay can be tolerated. Thus, time symmetry alone cannot be practical for networks with large and dynamic multicast groups. Given such vulnerability and the focus of the analysis on the scalability property of TAM, we have deemed it useless to pursue time asymmetric schemes as baseline for comparison. The flat multicast approach mimics the secret information asymmetry and thus more or less captures the fundamental idea of relevant previous work

B. Analysis for TAM

In TAM, the multicast involves distinct procedures for intra and inter-cluster operations. For the intra-cluster multicast, the cluster head forwards the packet over a tree

and employs a time asymmetry based authentication protocol that requires only a single MAC per packet. Again assuming d-balance tree, the bandwidth overhead can be calculated in a similar manner to the baseline approach above with the exception that the number of nodes is a fraction of the network population and the fact that the bit overhead per packet is much smaller. For a multicast that extends outside the source’s cluster, an inter cluster procedure is invoked to deliver the packet to the cluster heads of the participating receivers. Each cluster-head will then locally multicast the packet within its cluster. Thus, the number of transmissions is the sum of all local (intra-cluster) multicasts inside the individual clusters and the multicast from the source node to the other cluster-heads in the network.

Configuring TAM:

Both security and performance factors have to be considered when employing TAM. With respect to resilience to impersonation and replay attacks, TAM limits the effect of a node compromise to within a cluster. If a cluster member is captured, the TESLA-based intra-cluster authentication will deem any attempt by an adversary to launch these attacks ineffective. Meanwhile, the vulnerability to these attacks due to the capture of a CH node is still limited to within the cluster since only the key share of the compromised CH node will be uncovered and the adversary will not be able to fool other cluster-heads. However, a compromised CH cannot be prevented from launching impersonation and replay attacks against the members of its own cluster. Although the probability of capturing a CH is significantly low given the low CH count within the node population, it is advisable to have small clusters in order to mitigate the effect when it happens.

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

[1] C. E. Perkins, Ad Hoc Networking. Addison-Wesley, 2001.

[2] H. Yang, et al., “Security in mobile ad-hoc wireless networks: challenges and solutions,” IEEE Wireless Commun. Mag., vol. 11, no. 1, pp. 1536–1284, Feb. 2004.

[3] Y. Challal, H. Bettahar, and A. Bouabdallah, “A taxonomy of multicast data origin authentication, issues and solutions,” IEEE Commun. Surveys & Tutorials, vol. 6, no. 3, pp. 34–57, 2004.

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

[5] R. Canetti et al., “Multicast security: a taxonomy and efficient constructions,”in Proc. 1999 IEEE INFOCOM.

[6] R. Safavi-Naini and H. Wang, “Multi-receiver authentication codes: models, bounds, constructions, and extensions,” Inf. Computation, vol.
151, no. 1–2, pp. 148–172, May 1999.

[7] Perrig, et al., “Efficient and secure source authentication for multicast,”in Proc. 2001 Network Distributed System Security Symposium.

[8] A. Perrig, “The BiBa one-time signature and broadcast authentication protocol,” in Proc. 2001 ACM Conf. Computer Commun. sSecurity.

[9] L. Reyzin and N. Reyzin, “Better than BiBa: short one-time signatures with fast signing and verifying,” in Proc. 2002 Australian Conf. Info.Security Privacy, pp. 144–153

[10] A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, and P. Spilling, “A survey of key management in ad hoc networks,” IEEE Commun. Surveys & Tutorials, vol. 8, no. 3, pp. 48–66, Dec. 2006.

[11] F. R. Yu, H. Tang, P. Mason, and F. Wang, “A hierarchical identity based key management scheme in tactical mobile ad hoc networks,” IEEE Trans. Netw. Service Management, vol. 7, no. 4, pp. 258–267,Dec. 2010.

[12] R. Gennaro, et al., “Strongly-resilient and non-interactive hierarchical key-agreement in MANETs,” in Proc. 2008 European Symp. Research Computer Security. 293–303, 2002.