Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Two-Tier Authentication Scheme of Multicast Traffic for Large Scale AD-HOC Networks

K.Vidhyavathi[1] , M.Prabhakar [2]
Dept of CSE & JNTUA
Hyderabad, India

Abstract-- ***Multicasting style of communication in Ad-hoc networks are becoming an effective tool for many applications. These applications require security goals such as authenticating the source and integrity of message. Due to dynamic nature of ad-hoc network and unguaranteed connectivity make these inappropriate. A new approach Two-Tiered Authentication scheme for Multicast traffic for large scale ad-hoc networks has been proposed. This approach uses the time asymmetry, secret information asymmetry and Message authentication code to provide security over networks. This approach uses central authority for key management in ad-hoc networks. This approach will provide security and reliability over the network.***

Keywords: Multicast communications, Message authentication, Ad-hoc networks, Central Authority, Time asymmetry, secret information asymmetry.

I. INTRODUCTION

Higher flexibility and scalability in Ad-hoc networks motivates many applications. Nodes in ad-hoc network are self-organized these will require higher security over network. Due to limited commutation and communication resources it becomes difficult to provide security for ad-hoc networks. Group communication is common for ad-hoc networks which require data to be transmitted in a secure and trusted manner. To provide network security has to achieve security goals: (1) Confidentiality, to prevent unauthorized person from reading transmitted data, (2) Message authentication, to prevent tampering with transmitted packet, and (3) Source Authentication, used to prevent impersonating source by any receiver.

Source and message authentication is the corroboration that a message has not been changed and the sender of a message is as claimed to be. This can be done by sending a (1) Cryptographic digital signature, or (2) Message Authentication Code (MAC). The first involves asymmetric cryptography and often needs heavy computation both at the sender and the receiver. The latter involves creating a message and source specific MAC that can be verified by the receiver. Thus, the MAC implicitly ensures message and source integrity. In uni-cast, a shared secret key is used for MAC generation. Unfortunately, the use of a single shared key in multicast makes the group vulnerable to source impersonation by a compromised receiver. Dealing with multicast as a set of uni-cast transmissions each with a unique shared key is the most inefficient approach for addressing this concern. These issues combined with other constraints have made contemporary message and source authentication schemes used for multicast traffic in wired and single-hop wireless networks unsuitable for ad-hoc networks.

Many challenges are involved to provide group communication in ad-hoc networks. First, nodes in ad-hoc network have limited computing, bandwidth, and energy resources which make the overhead. Second, due to the unstable wireless links due to radio interference cause frequent packet loss errors and require a security solution that includes retransmission and replay over the packet loss. Third, use of same common key will make a problem of impersonating source by any receiver. So a solution has to be made for using multiple authentication keys over the network without overhead. This paper proposes a new two tier Authentication scheme of Multicast traffic for ad-hoc networks. Here nodes are grouped into clusters in order to cut overhead and provides scalability. Multicast traffic within the same cluster employs one-way hash chains to authenticate the message source. Message authentication code is appended to the message and the authentication key is revealed after the message is delivered which is used for authenticating source. 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. Cross-cluster includes message authentication codes (MACs) that are based on multiple keys. Each cluster has a distinct combination of MACs in the message in order to authenticate the source.

II. RELATED WORK

Many existing security solutions for conventional networks are ineffective and inefficient ad-hoc networks. Consequently, researchers have been working for the last decade on developing new security solutions or changing current ones to be applicable to Ad-hoc networks. In literature several approaches have been developed. Multicast security: Taxonomy and efficient constructions, in this approach 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 collision overheads and performance. Use of distinct

MAC per node will create bandwidth overhead and if same key is used it will make risk over nodes collision. Efficient authentication and signing of multicast streams over lossy channels TESLA is a very popular example of this category. One of the most distinct advantages of time asymmetry is the minimal per packet overhead that they impose. However, it requires clock synchronization among the communicating parties in order to prevent accepting forged packets, or discarding authentic packets. But for large networks forwarding delay will force the node to limit the packet transmission rate to avoid revealing next keys to intermediate nodes before all receivers get all previously transmitted packets. These shortcomings limit the scalability of these approaches for multi-hop networks where the maximum end-to-end delay varies significantly among receivers over time and space due to congestions and topology dynamics.

The BiBa one-time signature and broadcast authentication protocol. Few approaches fall in the third category, mixing both secret-information and time asymmetry. Such hybrid methodology opts to overcome the collusion vulnerability of secret information asymmetry and the tardy verification process of time asymmetry. Basically, a large set of keys is used and only a small subset gets involved in generating the MAC of a particular packet. The subset of keys is picked as a function of the message and is revealed in the same packet. Receivers verify the authenticity of the source as soon as the packet arrives. Since over time a receiver can eventually know all keys, the source periodically employs new keys. Unlike TAM, these schemes will not scale when used in multicast sessions with high packet transmission rates.

Security in wireless ad hoc networks is hard to achieve due to the vulnerability of links, limited physical protection, and the absence of a centralized management point. In this paper a distributed public key authentication service to protect the network containing malicious and conniving nodes.

III. SYSTEM MODEL

An ad-hoc network is a collection of autonomous nodes that together set up a topology without the support of a physical networking infrastructure. Ad-hoc networks will include several nodes for communications, among which nodes are via hop-by- hop routes using Omni directional wireless broadcasts with limited transmission range. Here nodes are grouped into clusters. The clusters formation can be based on location and radio connectivity. 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 clusters. Each cluster is controlled by a cluster-head. These will be reachable to all nodes in its cluster, either directly or over hop-by-hop paths. 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 neighbours. 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 focused. Figure (1) shows the example of the network clustering. Cluster heads are responsible for sending packets over hop-by-hop in the network. Nodes that have links to other clusters serve as gateways.

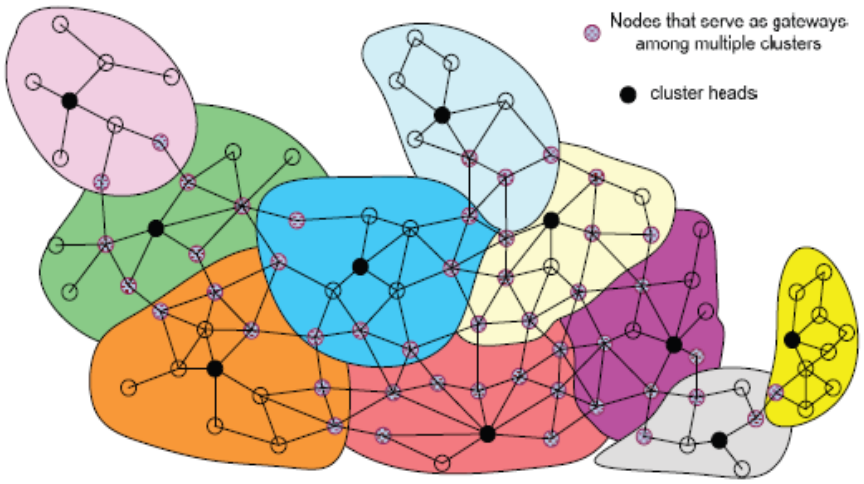

Fig.1. An example clustered ad-hoc network where each node is reachable to its cluster head via hop-by-hop. Nodes that have links to other clusters serve as gateways.

A. Key management:

Authentication can be provided based either on public-key or symmetric cryptography. In the former case, nodes issue digital signatures associated with the routing messages. Signatures can be verified by any other node, providing a secure proof of the identity of the sender. Digital evidence with similar properties can be constructed using secret-key cryptography, such as MACs (Message Authentication Codes). Key management in Ad-hoc networks is generally more difficult than in classical wired networks due to the absence of any infrastructure or central administrative authorities. So an central authority is used for key management system and is spread out to a subset of the mobile nodes. Tired authentication is possible because of multicast protocol. MAC is used for the authentication purpose of data integrity and

source authenticity. We generate a new network topology model called Central Authority (CA) to keep track of all the receivers in the Ad-Hoc network. The keys are necessary to authenticate the messages between the users. The message with MAC is transferred by the sender and received by CA. Whenever CA acknowledged the file then it distributes the file to all the nodes in the Ad-Hoc network as shown in Figure 2.

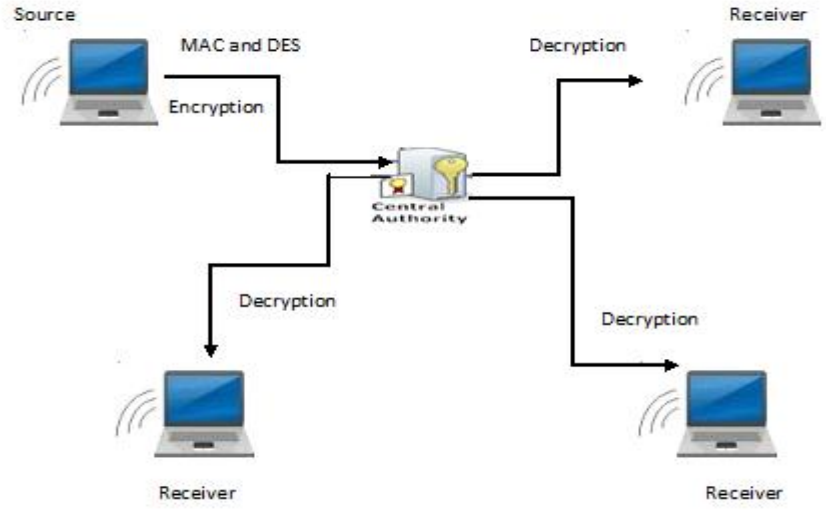

Fig.2 Overall model for the Central Authority

IV. AUTHENTICATION SCHEME 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. Clustering is a popular scheme for supporting scalable network operation and management.

A. Intra-cluster Authentication:

. For intra cluster authentication this model uses time asymmetry. Here one-way hash function is used to generate series of keys so that receiver can verify current key based on old key without being able to guess the future key. Initially sender picks a key K0 and generates a chain of keys by recursively applying a one-way function. These keys are used to generate MAC for individual packets. The source then reveals the last key K_l to all receivers which serves as base line for verification.

Sender constructs message packet P= $\{M|MAC(K_i,M)|K_{i+1}\}$ as shown in figure3.

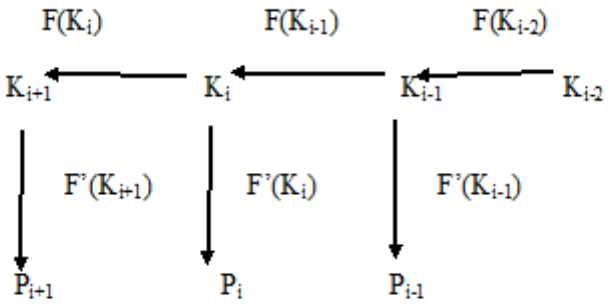

Figure 3: At the top of the figure, we see the one-way key chain (Derived using the one-way function F), and the derived MAC keys (Derived using the one-way function F')

Then receiver verifies the MAC using the series of authentication keys generated by hash function. So that source authentication is verified.

B. *Cross-Cluster Authentication:*

Authentication based on time asymmetry requires clock synchronization and thus does not suit for large networks. For cross-cluster multicast traffic uses secret information asymmetry and the cluster heads are responsible for authentication process. A third party person central authority (CA) distributes keys to source and all other cluster heads of designated receivers. Then source‘s’ belongs to $cluster_i$ multicast packet which contains data and MAC to all other cluster heads of designated receivers. Then cluster heads validates MAC using pre-distributed key and then forwards message packet to their designated receives.

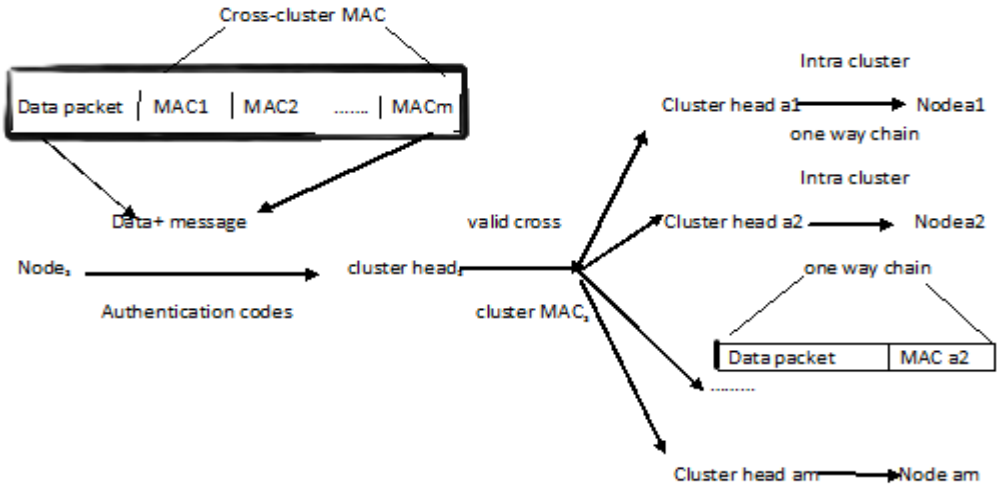

Fig-4: Packet transferring of intra and cross cluster over network.

Fig. 4 illustrates how TAM handles cross-cluster multicast traffic. Source node will send message along with MAC to Cluster head with in cluster. Then these cluster head will forward packet to other cluster heads which verifies MAC based on secret information asymmetry. These cluster heads will transmit packet to designated receivers by using time asymmetry.

V. RESULT ANALYSIS

This section describes the result analysis based on the performance evaluation As an expected result of this model will increase the performance of existing system In conclusion, the performance favours fewer clusters count, and dense and highly connected clusters. The main advantage over this proposed method performance evaluated by the central authority is lesser than the previous existing method.

VI. CONCLUSION

In recent years the use of ad-hoc networks in security-sensitive applications have been increased. The collaborative nature of these applications makes multicast traffic very common. Securing such traffic is of great importance, particularly authenticating the source and providing integrity of 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 a two tired hierarchical strategy combining both time and secret-information asymmetry in order to achieve scalability and resource efficiency. The key sharing through central authority in this paper increases the performance in the network. Our future work plan includes the study of enhanced guarantee for key sharing.

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] J. Y. Yu and P. H. J. Chong, "A survey of clustering schemes for mobile ad hoc networks," IEEE Commun. Surveys & Tutorials, vol. 1, no. 1, pp. 31–48, 2005.
[5] P. B. Velloso, et al., "Trust management in mobile ad hoc networks using a scalable maturity-based model," IEEE Trans. Network Service Management, vol. 7, no. 3, Sep. 2010.
[6] L. Junhai, Y. Danxia, X. Liu, and F. Mingyu, "A survey of multicast routing protocols for mobile ad-hoc networks," IEEE Commun. Surveys & Tutorials, vol. 11, no. 1, pp. 78–91, first quarter 2009.
[7] K. Marzullo and S. Owicki, "Maintaining the time in a distributed system," in Proc. 1983 ACM Symposium Principles Distrib. Computing.
[8] R. Canetti et al., "Multicast security: a taxonomy and efficient constructions," in Proc. 1999 IEEE INFOCOM. [9] Perrig, "The BiBa one-time signature and broadcast authentication protocol," in Proc. 2001
[9] Mohamed Younis, Osama Farrag, Bryan Althouse "TAM: Tiered Authentication of Multicast Protocol in Ad-hoc Networks" in IEEE Transactions On Network And Service Management, Vol. 9, No. 1, March 2012

