Hybrid Authentication Model for Multicast Protocol in AD-HOC Networks

J.Siva Kumar[1], Boppudi Swanth[2], Betam Suresh[3]

[1]pursuing M.Tech(CSE), Vikas Group of Institutions (Formerly known as Mother Theresa Educational Society Group of Institutions), Nunna, Vijayawada, Affiliated to JNTU- Kakinada, A.P, India

[2]working as an Assistant Professor in Department of CSE at Vikas Group of Institutions (Formerly known as Mother Theresa Educational Society Group of Institutions), Nunna, Vijayawada, India.

[3]working as an HOD at Vikas Group of Institutions (Formerly known as Mother Theresa Educational Society Group of Institutions), Nunna, Vijayawada, Affiliated to JNTU Kakinada, A.P , India.

***Abstract*—These Ad-hoc networks are an efficient tool for many applications such as military field, situational awareness, etc. Hence these applications are divided based on the environment that they serve in and by the multi style of communication traffic. Therefore, securing the source node and providing the mediator of the message traffic to become a basic requirement for the operations and maintenance of the network. However, the limited computational and communication resources, the large scale deployment and the unguaranteed connectivity to valid securities make correct solutions for wired networks and as well single sided wireless networks. In this document shows a one new methodology known as Tired Authentication scheme for Multicast network traffic (i.e, TAM) for a large scale ad-hoc networks. This new authentication model represents the advantages of the time asymmetry and the secret information asymmetry techniques, Using this we can send a message or file from source node to the destination node without effecting any unauthorized attacks on particular file in an one-way hash function chain in order to maintain and authenticate the source node messages, Whereas using a mechanism called cross-cluster multicast traffic indicates that the message authentication codes i.e., MACs that are based on a set of keys to generate a key at source node and that generated key should match with the destination node key then only that transferred message should be reached to the destination node otherwise it cannot, By using this TAM we can reduce the wireless network problems such as in civil and military areas etc.**

***Keywords*— Ad-hoc networks, Multicast network, secret information, message authentication codes.**

Introduction

In wireless technologies the enabled networked solutions for many nonconventional military and civil applications. In these recent years, the ad-hoc networks has been increased attention from the research and engineering community, and it has motivated by different types of applications like asset tracking, digital battlefield and border protection etc. In all these network applications it is important to manage the efficient network suitable nodes. In addition to that the solutions must be secure and scalable to support networks manages vast areas with large set of network nodes that communicates over many hops. And the main issue in these ad-hoc networks are if and only if consider the communication is group communication is a very critical in ad-hoc networks due to their inherently collaborative operations, means that where the nodes co-operate in network management and strike to achieve common missions autonomously in highly unpredictable environment without changing on infrastructure equipment. For example, consider X-it is a source node and Y-is a destination node, X wants to send some confidential data to node Y, X sent data to Y at that time these ad-hoc networks searching for a wireless network for transferring that particular file destination for that it first discover a route for sending from X to Y and also it will control the traffic such as route discovery to setup multi-hop paths, the establishment of time synchronization etc. such that the data from X to Y has to be delivered in a secure and trusted manner.

The following security features are like Confidentiality- to prevent unauthorized people from reading the transmitted data, Message integrity, to prevent tampering with transmitted messages and Source Authentication-using this we can prevent the man-in-the-middle attack that may replay transmitted data node identification. However here confidentiality is achieved by encrypting the transmitted data. The main aim of presenting this paper is for achieving the principles like the Message integrity and Source authentication. Providing an efficient multicast message and source authentication security service that can be easily scale for large networks, it is a main capability for the operation and management of the network.

Sending a data from source to destination, at source side message authentication is the collaboration that a message has not been changed and the source of a message is claimed to

be. This can be achieved by sending a Cryptographic digital signature, and a 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 unicast, 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 unicast 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.

Here we have two types of goals implemented in this paper those are.

1. What are the challenges and Design goals implemented in this paper are: The main challenge in ad-hoc networks that make multicast authentication with multiple factors, the issues are fundamentally due to the resource constraints and the wireless links. In this the nodes have some limited computational, energy resources and bandwidth which make the basic asymmetric key using cryptography methods. In order to loss the packet due to unstable wireless links, for that we require a security solution that can get the missed packets and as well the differentiate between packet retransmission and replay.

In order to being a resource efficient and robust to packet loss, a security solution should be for large scale group of destinations and along with multi-hop paths.

2. This paper also shows that a new Tired Authentication scheme for multicast traffic for ad-hoc networks (TAM). 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 its authenticate the source node and then to deliver the data/message to the destinations using intra cluster authentication scheme. Here the TAM integrates the advantages of the secret information asymmetry and the time asymmetry mechanisms

Related Work

Here in this, the source authentication schemes found in the literature can be divided into 3 categories those are:

1. Secret information asymmetry.
2. Hybrid asymmetry and
3. Time asymmetry.

The asymmetry denotes that the destination node can verify the message origin using the MAC in a packet, without knowing how to create the MAC. In this the asymmetry property is the key for providing unauthenticated of data sources. In secret information asymmetry each and every node is assigned a share in a secret, Example. a set of keys. A source node appends MACs for the multicast keys so that the a receiver verifies the authentication of message without being able to merge the MACs for the other nodes.

The main purpose of time asymmetry is to tie the validity of the MAC to specific time duration so that a duplicate packet can be discarded. Half-duplex (one-way) hash chains are usually to generate a series of keys so that a destination can verify the current key based on old key without being able to identify the future key. Initially at source side, source takes a key key0 and generates a by chain of key by repeatedly applying a one-way (half-duplex) hash method. These keys are used to form the MAC for the individual message packets. And to achieve a full-duplex(two-tiered) authentication method for sending a message from source to multiple destination nodes we have a mechanism called TAM For example, in monitoring the traffic within a cluster is used by the member nodes to build mutual trust that is considered, along with public certificates, sufficient for authenticating the source of a transmission. For inter-cluster communication public key certifications are used to find out the trust level of the source. The receiver asks a number of introducers within the source cluster to provide the certificate for the source and to share their assessment of its trust level. The introducers sign their reply messages using their private

keys to make the certificate valid. Given the overhead for public key cryptography, this approach obviously does not scale well for large multicast groups. In addition, a node that served on a multicast group cannot be virtually evicted from that group without avoiding it while routing the multicast traffic. Meanwhile it have a proposed a message/packet authentication protocol called GSA that represents a efficiently deal with dynamic modifications in the topology in a vehicular network and also it shows some fact that in some applications, i.e, for example consider in military applications vehicles can naturally grouped due to shared movement pattern. And the each group in military is assigned to a leader to act as a trust authority. In this the group leader is responsible for multicasting commands to all the group members and interfacing its groups to other groups in the network, and also it uses a group attributes to generate a authenticated key for intra-group message traffic. Here the TESLA is a mechanism to apply for inter-group authentication like TAM; GSA adopts different security mechanisms for intranet and internet communications.

Here we have some of the techniques using by TAM are.

1. Key Management in Wireless Ad Hoc Networks: Collusion Analysis and Prevention

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, 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. Simulation results have demonstrated that our proposed solution significantly boosts the network resilience to potential collusion threats.

2. Efficient and Secure Source Authentication for Multicast

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.

3. Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model:

In this paper, we 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 multi-hop 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.

And also this paper presents two types of models those are

A.**Trust and threat model**

Assumed that here cluster heads to have public key certificates assigned identity based asymmetric keys generated by a common trusted authority.

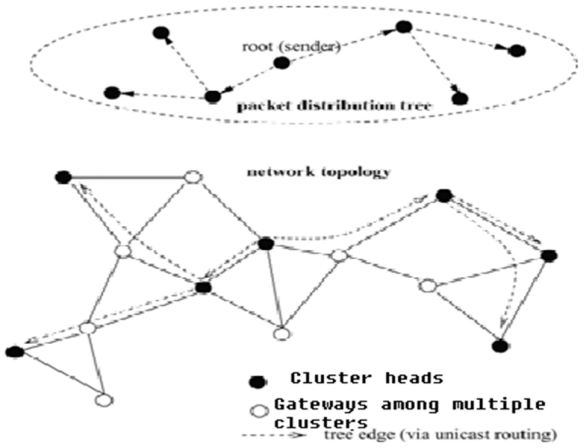

Fig:1. An example clustered ad-hoc network where each node is reachable to its cluster head via at most 1-hop (2-hop clustering. Nodes that have links to other clusters serve as gateways.

These public keys can be used to form clusters securely and bootstrap TAM. Alternatively, if public key certificates are not suitable, TAM may employ a robust technique to bootstrap mutual trust among the individual nodes. We aim to eliminate any need for interaction with the authority to retrieve the public key of some nodes in the network. TAM bootstrapping will be needed at the time sessions are established and during the formation of a new cluster. Basically, as detailed in Section IV, the source uses asymmetric cryptography to deliver the session keys to the main players in the authentication process. All nodes are to be preloaded with a known one-way hash cryptographic function. The function should be proven secure with extremely low probability that an adversary can determine the input to the function given its output. This paper mainly considers an adversary who tries to manipulate the system through capturing and compromising some nodes. When a node is captured, its memory can be read or tampered with. Therefore, an adversary would know the keys of a compromised node. In addition, the operation of a compromised node may be manipulated to launch attacks such as replay, impersonation, etc... TAM opts to ensure source and message authentication in order to counter modify, replay and impersonation attacks. Other attacks are beyond the scope of this paper.

B. **Architectural Model**

A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data.

An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of IEEE 802.11 wireless networks.

TIERED AUTHENTICATION OF MULTICAST TRAFFIC
The main purpose of TAM is a two-tier authentication process for multicast traffic in ad-hoc networks. It uses clustering to divide a network and then authenticates the multicast traffic by maintaining time asymmetry for intra-cluster traffic and secret information asymmetry for inter-cluster traffic. This process of TAM is explained in below.

Intra-cluster authentication- The main idea of this is to group the nodes into clusters enables having a reasonably tight bound on the end-to-end delay of packet delivery and will enable the use of a time asymmetry based authentication technique. Intra-cluster authentication in TAM is based on TESLA. In inter cluster multicasting traffic will be secured differently means that a dource node generates a chain of one-time-use keys using

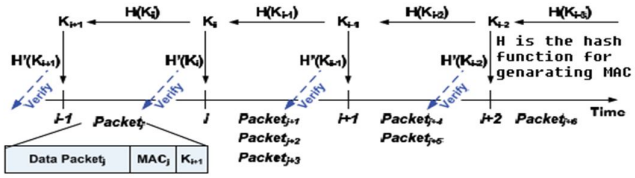

Fig: 2. A source used a key Ki during period j and reveals it in period j +1. Thus, a packet in period j will have a MAC based on Ki and will also include Ki + 1 for authenticating the packet received in period j − 1.The hash function. Example above shows that the MD5, SHA1 etc. and shares only that the last generated key *KI*. With the destination a message can be secured only when the used key in the chain of actions. The above figure shows that the authentication process to verify the authentication key, at destination side it uses repeatedly applies the cryptographic hash function until it reaching *KI*. Finally the receiver can stops when reaching a key that has been used previously. A key that cannot be used outside its time interval and the message will be ignored if the MAC is based on an expiry key. This approach has two main advantages they are.

> The MAC over header is small; basically a one single MAC is used per every multicast packet for all receivers.

> A missed key in a lost packet would not be authentication process since a destination can send acknowledgement back to *KI*.

In TAM, it consider about the authentication delay is generally addressed by the fact the cluster includes just a subset of the network nodes. The maximum end to end delay is experienced by an intra-cluster multicast will be mostly dependent on the cluster radius, by controlling these cluster radius of the cluster at the time number of hopes between a member node and the cluster-head.

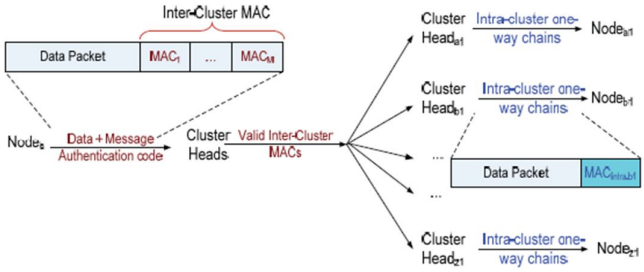

Fig: 3 Illustrating the steps and packet contents when a node "s" multicast. A data packet to nodes "a1", "b1", · ·. , "z1" according to TAM.

Inter-cluster Authentication:

This is typically based on asymmetry requires clock synchronization and does not suit for 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. Here 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 i, j, k and m, node S sends the some message to the clusterC_I, C_J, C_k and C_m. These cluster heads will then forward the message to receivers in their clusters. The process shows that the source will generate a pool of M keys; each of the N_{CL} clusters in the network will be assigned a share L of keys, with M < L ×N_{CL}. 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 toN_{CL}.

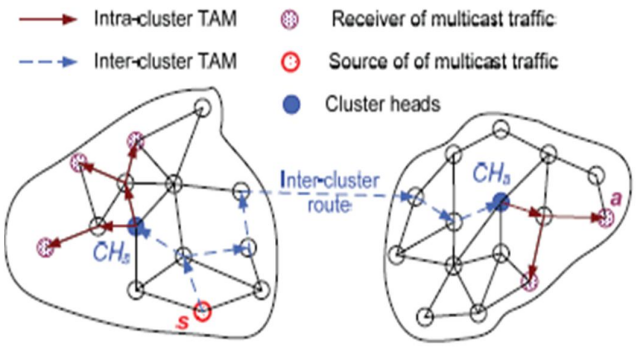

Fig: 4. Summary of the TAM inter-cluster operation. Delivery of the multicast message from a source "s" to all cluster heads applying the TAM inter-cluster authentication, and from each cluster-head, of the designation clusters $CH_s$and $CH_a$to the target node "a" apply the TAM intra-cluster protocol.

Let $K_j^{inter,s}$ be the j^{th} out of the M keys that a source node "S" generates for inter-cluster authentication and H be a secure half-duplex hash cryptographic function and $K_j^{inter,s}$ is calculated through repeated application of the H via root secret key $K_0^{intra,s}$ = H($K_l^{intra,s}$), with $K_l^{intra,s}$ = H(H(…(($K_0^{intra,s}$))…))

1. Source "S":

> Inter- cluster packet payload

P=Data\MAC (Data, $K_l^{inter,s}$), MAC (Data, $K_l^{inter,s}$),.., MAC (Data, $K_l^{inter,s}$)

> Node "S" forwards the inter-cluster packet to cluster heads, CH_s, CH_a, etc, over an inter-cluster head multicast tree.

2. CH_a (Similarity for CH_s and other cluster heads):- -Extract the MAC corresponding to its key share (total of L, e,g., $K_j^{inter,s}$,j=1,…L)

--Verify MAC (Data, $K_j^{inter,a}$) $\forall_j$= 1,… ,L

--$Packet_a$ = Data | MAC (Data, $K_q^{intra,a}$) | $K_{q+1}^{intra,a}$| Header

--CH_a Multicast $Packet_a$ to local receivers that are members of the multicast group of the source "S"

3. Receiver "a" in the cluster ofCH_a:

--Wait for a packet from CH_a that contains $K_q^{intra,a}$

--Verify that $K_{q+1}^{intra,a}$=H ($K_q^{intra,a}$)

--Verify MAC (Data, $K_q^{intra,a}$)

Higher values of L allow cutting the overhead by assigning unique key combinations to cluster heads (M =$LogN_{CL}$), 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 [14]. It is worth mentioning that N_{CL}would depend on the cluster radius and the used clustering algorithm.

CONCLUSION

Nowadays the people are using internet in the use of ad-hoc networks with security applications such as military, digital battlefield. The main theme of these security applications makes multicast traffic very common in these days so to secure such traffic is very great issue, mainly authenticating the source node and message to prevent any un-authorization attacks by an intruder. This topic deals with TAM, which is a two way hierarchical for combining both time and secret information asymmetry in order to get secure and scalable; the performance of TAM has been analyzed functionally and through simulation. And our future work includes the effect of different clustering strategies on the performance of TAM.

REFERENCES

C. E. Perkins, *Ad Hoc Networking*. Addison-Wesley, 2001.

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.

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.

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*.

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

AUTHORS PROFILE

J.Siva Kumar, Pursuing M.Tech(CSE) from Vikas Group Of Institutions (Formerly known as Mother Theresa Educational Society Group of Institutions), Nunna, Vijayawada. Affiliated to JNTU-Kakinada, A.P., India

Boppudi Swanth, working as an Asst. Professor at Vikas Group Of Institutions (Formerly known as Mother Theresa Educational Society Group of Institutions), Nunna, Vijayawada. Affiliated to JNTU-Kakinada, A.P., India

Betam Suresh, is working as an HOD, Department of Computer science Engineering at Vikas Group of Institutions (Formerly Mother Teresa Educational society Group of Institutions), Nunna, Vijayawada, Affiliated to JNTU-Kakinada, A.P., India