Cluster Based Secure Data Broadcast of CLAODV Protocol for MANET
P. Indumathi
(Teaching fellow, Dept of CSE, Anna university, India)

ABSTRACT— Ad-hoc Networks are using multicast protocol to broadcast the messages. Multicast authentication in ad-hoc networks are very challenging based on below mentioned multiple factors such as nodes have limited computing, bandwidth, and energy resources. Additionally, frequent packet loss errors require a security solution that can tolerate missed packets. The existing cryptography techniques are inefficient for multicast traffic patterns. Since using a common key for all receivers will make it relatively easy to impersonate a sender by any one of the receiving nodes. The proposed system exploits network clustering and routing technique in order to cut the overhead and ensure scalability. Multicast traffic in intra cluster using one-way hash chains to authenticate the message source. In the inter cluster, (i.e. cross cluster) multicast traffic includes message authentication codes that are based on multiple keys. In order to authenticate the source, each cluster uses a unique subset of keys to looks for its distinct combination of message authentication codes in the message. 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.

Keywords— Multicast communications, Message authentication, ad-hoc networks.

I. INTRODUCTION

A "Mobile Ad Hoc Network" (MANET) is an autonomous system of mobile router and associated hosts connected by wireless links-the union of which form an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Ad Hoc networking is one of the most vibrant and active "new" fields today.

Group communication is challenge operation in ad hoc networks because of their unpredictable environment. But Multicast is an efficient method to realize group communications. However, there is a big challenge in enabling efficient multicasting over a MANET whose topology may change constantly. So the multicast uses clustering to partition a network and then authenticates multicast traffic. So the nodes has to be delivered the data packet in a secure and trusted manner.

The network services need to provide the following security goals: (1) Confidentiality, to protect data from unauthorized disclosure, (2) Message integrity, to prevent tampering with transmitted messages, and (3) Source authentication, assurance that the communicating entity is the one that it claims to be. In this paper aims at addressing the second and third goals. Message integrity use asymmetric cryptography and often needs heavy computation both at the source and destination. The source authentication involves creating a message and source specific MAC that can be verified by the receiver.

In this paper proposes source and message authentication scheme for multicast traffic for MANET. It exploits network clustering and routing technique in order to cut the overhead and ensure scalability. In the intra cluster employs one-way hash chains to authenticate the message source. The authentication code is combined with message body are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the same secret key, to generate a new MAC. On the other hand, Inter cluster multicast traffic includes Message Authentication codes that are based on multiple keys. To authenticate the source, each cluster use unique combination of MACs in the message. At the time of initiating the multicast session the pool keys are generated by the sender. The keys will be securely transmitted to the head of every cluster that hosts one or multiple receivers. After that the sender transmits the messages to the head of the individual cluster. The cluster head authenticate the intended recipient using the intra-cluster authentication scheme and then deliver the message.

II. RELATED WORK

Ahmed Y. Al-Dubai et al [1] proposed a novel path-based multicast algorithm for interconnection networks. The Qualified Group is the first multicast algorithm that considers the multicast latency at both the network and node levels across different traffic scenarios in interconnection networks. The proposed multicast algorithm exhibits superior performance characteristics over other well-known path-based multicast algorithms under different operating conditions. In addition, the results show that the QG can significantly improve the parallelism of the multicast communication.

M. Anupama and Bachala Sathyanarayana [2] analyzed and compare some of existing works on clustering in MANETs. The highly dynamic and unstable nature of MANETs makes it difficult for the cluster based routing protocols to divide a mobile network into clusters and determination of cluster heads for each cluster. Categorize the works as Location based, Neighbor based, Power Based, Artificial Intelligence Based, Mobility based and Weight Based. The advantages and disadvantages of these techniques and suggest a best clustering approach based on the observation.

Eric Astier1, Abdel hakim Hafid et al [3] proposed a mesh-based multicast protocol, called centered protocol for unified multicasting through announcements (CPUMA), that achieves comparable reliability as existing mesh-based multicast protocols, however, with significantly much less data overhead. In CPUMA, a distributed core-selection and maintenance algorithm is used to find the source-centric
center of a shared mesh. The proposed centering scheme
allows reducing data packet overhead and creating
forwarding paths toward the nearest mesh member instead of
the core to reduce latency.

a cross-layer design. CLD based architecture is proposed,
where the objective is to provide a solution for power
conservation, congestion control, and link failure
management. The link quality is determined by the received
signal strength at the physical layer. The channel
interference, contention and RTS/CTS packets of the MAC
layer are used to determine the transmitting power and ensure
the Quality of Service at the application layer.

Mohamed Younis, Osama Farrag, and Sookyoung Lee [5]
proposed a novel methodology that combines network
clustering and mesh-based multicast routing. The Cluster-
Mesh based Multicast Routing (CMMR) methodology forms
a backbone using cluster-heads. This makes the backbone
more stable against frequent node mobility and enables
scalability by limiting the scope of the core maintenance.

F.Richard Yu et al. have exploits the hierarchical
structure of a network for key management [6]. The proposed
scheme can select the best nodes to be used as PKGs from all
available ones considering their security conditions and
energy states. Security state can change dynamically; some
nodes may be in a safe state while others may be under attack
by adversaries. The nodes with master key shares, these
nodes would be compromised, and the security of the whole
network is breached when a threshold number of
shareholders are compromised. Selecting a node under attack
or a compromised node to function in the PKG process
would pose a risk to the network security.

X. Xiang, X. Wang, and Y. Yang [7] proposed a novel
Efficient Geographic Multicast Protocol (EGMP). EGMP
uses a virtual-zone-based structure to implement scalable and
efficient group membership management. A network wide
zone-based bidirectional tree is constructed to achieve more
efficient membership management and multicast delivery.
The position information is used to guide the zone structure
building, multicast tree construction, and multicast packet
forwarding, which efficiently reduces the overhead for route
searching and tree structure maintenance.

III. PROPOSED METHODOLOGY

In this paper proposes a new source authentication
scheme for multicast traffic for MANET. In the proposed
methodology exploits network clustering and provide secure
routing in order to cut overhead, ensure scalability and
improve source authentication. Fig 1 explains the system
architecture of proposed methodology.

1. Clustering

Clustering is an important research topic for MANET
because clustering makes it possible to guarantee basic levels
of system performance, such as throughput and delay, in the
presence mobility and a large number of mobile nodes. The
process of dividing the network into interconnected
substructures is called clustering and the interconnected
substructures are called clusters. The cluster head (CH) of
each cluster act as a coordinator within the substructure. The
cluster head coordinates the cluster activities inside the
cluster. The ordinary nodes in cluster have direct access only
to cluster head and gateways. The nodes that can hear two or
more cluster heads are called gateways.

Each CH acts as a temporary base station within its zone
or cluster. It also communicates with other CHs. The Cluster
based routing provides an answer to address nodes
heterogeneity, and to limit the amount of routing information
that propagates inside the network. The grouping of network
nodes into a number of overlapping clusters is the main idea
behind clustering.

1.1) K-Mediod Clustering:

The k-means method uses centroid to represent the cluster
and it is sensitive to outliers. This means, a data object with
an extremely large value may disrupt the distribution of data.
K-medoids method overcomes this problem by using
medoids to represent the cluster rather than centroid. A
medoid is the most centrally located data object in a cluster.

Here, k data objects are selected as medoids to represent k
cluster and remaining all data objects are placed in a cluster
having medoid nearest (or most similar) to that data object.
After processing all data objects, new medoid is determined
which can represent cluster in a better way and the entire
process is repeated. Again all data objects are bound to the
clusters based on the new medoids. In each iteration, medoids
change their location step by step. Or in other words, medoids move in each iteration. This process is continued until no any medoid move. As a result, \( k \) clusters are found representing a set of \( n \) data objects. The working principle of K-Mediod is explained in the Fig. 2. An algorithm for this method is given below.

1. Initialize: select \( k \) of the \( n \) data points as the medoids.
2. Associate each data point to the closest medoid.
3. For each medoid \( m \)
   i. For each non-medoid data point \( o \)
   ii. Swap \( m \) and \( o \) and compute the total cost of the configuration.
4. Select the configuration with the lowest cost.
   i. Repeat steps 2 to 4 until there is no change in the medoid.

Step 2: When receiving packet by neighbor nodes, it calculate the received signal strength. Information.

Step 3: The received signal strength information is used to compute path loss incurred to choose reliable links by monitoring the signal quality to judge which route is chosen in the route discovery process.

Step 4: Calculate path loss

\[
\text{Path loss} = PT - PR
\]

Where PR is Received Power of receiver and PT is Transmission Power of sender.

Step 5: Checks whether its transmission power of sender is greater than the sum of path loss and receiver threshold.

If yes, accept the Route request packet

Otherwise

Discard the route request packet.

Step 6: Repeat step 2 to 5 until reached the receiver node.

Step 7: Finally discover the route between sender to receivers.

3. source Authentication of Multicast Protocol

In the proposed system provide the source authentication in ad-hoc network for two ways. Initially, clusters the partitioned network, and then authenticates multicast traffic by employing time asymmetry for intra-cluster traffic and secret information asymmetry for inter-cluster traffic.

3.1) Intra-Cluster Source Authentication:

In the intra cluster, sender and receiver nodes present in the same cluster. 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, \( K_i \), with the receivers. A message can be authenticated only when the used key in the chain is revealed. Fig. 3 demonstrates the authentication process. To verify the authentication key, the receiver recursively applies the cryptographic hash function until reaching \( K_i \). 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 \( K_i \).
clusters in the network will be assigned a share of keys, with \( M < L \times N_c \). 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 CH 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 CH 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 \( N_c \).

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.

3.2) Inter-Cluster Source Authentication:

In the inter cluster, when sender node identified the receiver from another cluster, then sender generated number of keys to each cluster’s header nodes. Basically, the source “s” that belongs to Cluster 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 \( CH_g, CH_h, CH_j \), and \( CH_k \). These cluster heads will then forward the message to the receivers in their respective clusters. 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.

The source will generate a pool of \( M \) keys. Each of the \( N_c \) nodes of the multicast group of a source node “s” includes nodes “a1,” “b1,” . . . “z1”.

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. This project pursues a two-tier hierarchical strategy combining both time and secret-information asymmetry in order to achieve scalability and resource efficiency. The performance of the proposed system has been analyzed mathematically and through simulation, confirming its effectiveness. The k-medoid cluster method is very effectively clustering the nodes with assist of distance between them. The cross layer ad-hoc on-demand distance vector routing method is efficiently discovering the route between the sender and receiver node. In this method the

---

**Fig. 3 MAC based Key generation in Intra-cluster and authenticates the packet**

**Fig. 4 Inter-cluster operation**
transmission and receiving power is measured so, the unidirectional links are avoided in the route request stage itself. CLAODV provide bidirectional link route to avoid link break efficiently.

The future enhancement includes studying the effect of different clustering strategies and enhances message authentication code generation method.

REFERENCES


Author

Mrs P.Indumathi did her B.E in Computer Science & Engineering from Arasu Engineering college, kumbakonam She did M.E (CSE) in M.N.M jain engineering college, Chennai. She has 3 Years of teaching Experience at Ramanujar engineering college and A.V.C engineering college in Mayiladuthurai. She has published about 5 papers in National Conferences. Now she is working in Anna University, chennai as a teaching faculty.