Single and Multi Hop Security Protocol for MANET

Shrinivas Karwa
Computer Department
VJTI,
Mumbai,India
shrikarwa1@gmail.com

Vishruti Desai
Computer Department
VJTI,
Mumbai,India
vishrutidesai@gmail.com

Ashwini Dalvi
Computer Department
VJTI,
Mumbai,India
ashwinidalvi@gmail.com

Dr.B.B.Meshram
HOD,Computer Department,
VJTI,
Mumbai,India
bbmeshram@vjti.org.in

***Abstract*— Mobile Ad hoc Networks (MANET) is self-organizing, infrastructure-less, multi-hop network. The wireless and distributed nature of MANETs and the very bad security environment in battlefield bring a great challenge to securing mobile ad hoc networks. Mobile nodes rely on each other to maintain the network connection This paper proposes a protocol for secure communication between end users in single and multihop mobile Ad hoc networks, based on clustering approach. This protocol is based on Public Key cryptography and Hash algorithm.**

***Keywords*— adhoc, cluster, singlehop, multihop, security**

I. Introduction

A Mobile Ad Hoc Network (MANET) is a network consisting of a collection of nodes capable of communicating with each other without help from a network infrastructure. As there is no defined topology it is very difficult to distinguish between insider and outsider node of MANET. Mobile Ad hoc network is characterized by some of the features like frequently changing network topology, presence of selfish nodes, incapable of executing heavy computation, power limitation, and storage limitation. Due to presence of above mentioned properties of MANET the implementation become a real challenge.

Due to nature of MANET the lack of an online CA or Trusted Third Party adds the difficulty to deploy security mechanisms. Nodes in MANET are incapable to execute heavy computation. In MANET any node can join the network, leave the network at point of time and can communicate with any other node; so authentication of communicating nodes before the transmission of actual data is a prerequisite. The proposed authentication protocol needs to consume low computational power and minimum delay.

In MANET, secure communication protocol should satisfy the following security requirements: [7] [8]

1. **Confidentiality:** Message information is kept secure from unauthorized party.
2. **Data Integrity:** Message is unaltered during the communication.
3. **Authentication:** Correct identity is known to communicating partner.
4. **Non-repudiation**: The origin of a message cannot deny having sent the message.

Section II tells us about the previous proposed protocols and their drawbacks. **Section III** suggests the new protocol for MANET security. It contains notations used in the protocol, actual structure of protocol and three cases of the protocol. **Section IV** deals with how the proposed protocol satisfies the above mentioned security requirement and paper concludes with conclusion **section V**.

II. Literature Survey

In this section, we describe two most relevant clustering schemes. Varadharajan V, Shankaran R and Hitchens M. [1] have proposed a protocol on security for cluster based adhoc networks, using timestamp concept. They use Public Key Infrastructure and Pre Key Distribution approach in their protocol. Pre key distribution approach is not suitable for MANETs due to its inherent nature of manual distribution of keys and scalability problems. Two phases are involved in their proposed protocol such as authentication and communication phase. When a mobile node joins the cluster head, it executes the authentication phase. When a node wants to communicate with another node, it executes communication phase. All the nodes share a secret key with their respective cluster heads. Each cluster head needs to share a secret key with other cluster heads. Storage overheads are much higher in this approach since cluster heads need to store the shared keys of all the nodes within its cluster and with other cluster heads.

Jung- San Lee and Chin-Chen Chang [2] have proposed protocol using node identities to provide secure communication for cluster – based ad hoc networks. Their protocol is based identity based scheme. It consists of two phases, such as *authentication* and *communication* phase. It consists of trusted third party (TTP), which takes care of generating and issuing the secret information to each involved node. When a node wants to join the cluster it has to get the authentication token from the cluster head by executing the authentication phase with the cluster head. TTP generates and distributes a secret key for each node and for each cluster head through a secure channel. Secret key is generated based on the timestamp and certificate is generated for each particular node is being generated by applying hash function on that particular node's secret key. Nodes, which are within one-hop distance in a cluster, can communicate directly with each other using identities of the opposite entities. As in one hop distance there is no need of intermediate node to forward the packet to destination node as both the Sender and Receiver are at one hop distance from each other. Cluster based approach is reliable and efficient in multihop which take use of intermediate nodes to forward the packet towards source and destination nodes. Since in the later case, source node needs to depend upon the intermediate nodes. These are completely dynamic and so it is difficult to maintain the stable link through the dynamic intermediate nodes from source to destination. If any node moves out from the established path of a particular link, again we need to initiate the path establishment process. This path reestablishment process takes considerable time to reestablish the route and resume the data transmission. In cluster-based approach, the cluster head ensures the reach ability and reliability features. Because of this, delay is reduced and the throughput probability is at the maximum.[6] Due to the above listed advantages, we propose this novel cluster based secure communication protocol for mobile adhoc networks.

III. Proposed protocol

A.Assumptions:

Cluster head does not maintain a database to store secret keys and identities of nodes within its range. Every time when a node wants to communicate with other node, it needs to execute the proposed protocol in order to provide secure communication based on the position of the destination i.e. with intra cluster or with inter clusters. Node belongs to only one cluster at a time.

B.Scenarios in Consideration:

We consider three different node's location specific scenarios in the proposed protocol.

1. Two communicating mobile belongs to same cluster are at one hop distance from each other.
2. Two communicating nodes are not within the transmission range of each other but are in the same cluster.
3. Two communicating nodes belong to different cluster.

C. Notations:

Final$_s$	(Final Source) Node s responsible for originating and sending the data.
Final$_d$	Final Destination) Node d to which data is sent.
CHi	Cluster Head i such that all nodes in that cluster are at one hop distance from CH
Ni	Node i which belongs to one and only one cluster.
Hash	Collision Resistant Hash function
M	Message that is send by the Final sender to Final destination.
T	Time stamp T shows details about time and date.
Si	Area of Cluster Chi
PBi	Public key of node i
PKi	Private Key of node i
R	Random Number

D. Format of Protocol:

Receiver's Public Key Final/Inter {Sender Identity Final/ Inter, Final Source, Final Destination, Sender's Private Key Final/Inter [Timestamp (T), Random Number (R), Message (M), Hash (M||T||R)]}

The inner packet "Sender's Private Key$_{Final/\ Inter}$ [Timestamp (T), Random Number (R), Message (M), Hash (M||T||R)]" is called as **Data packet**.

*a) Case1***:** *If both the nodes belong to one cluster and at one hope distant from each other.*

In Figure 1, Ni and Nj are two node that want to communicate with each other.

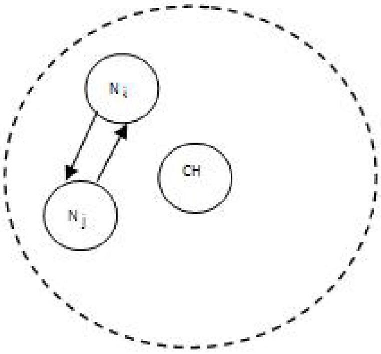

Figure 1: Nodes Ni and Nj belong to one cluster at one hop distance from each other.

*Protocol***:**

Ni→Nj
PBj{Ni, Ni, Nj, PKi[T, R, M, Hash (M| T||R)]}

Nj→Ni
PBi{Nj, Ni, Nj, PKj[T, R, M, Hash (M| T||R)]}

Case2: If both nodes belong to one cluster and at one *hope distant from Cluster Head but not at one hop distance from each other.*

In Figure 2, Ni and Nj are two node that want to communicate. CHk is cluster head such that node Ni and Nj are at one hope distant from Cluster

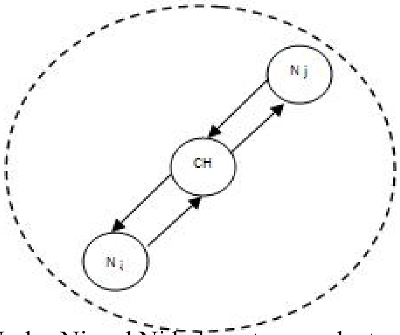

Figure 2: Nodes Ni and Nj belong to one cluster at one hop distance from cluster Head.

Protocol:

Ni→ CHk
PBk{Ni, Ni, Nj, PKi[T, R, M, Hash (M| T||R)]}

CHk→Nj
PBj {CHk, Ni, Nj, PK$_k$[T, R, M, Hash (M| T| R)]}

Nj→ CHk
PBk{Nj, Ni, Nj, PKj[T, R, M, Hash (M| T||R)]}

CHk→Ni
PBi{CHk, Ni, Nj, PK$_k$[T, R, M, Hash (M| T| R)]}

*Case3**:** If both nodes belong to different clusters and at one hope distant from cluster Head.*

Figure 3,Ni and Nj are two node that want to communicate which belongs to two different cluster. CHm is cluster head of node Ni. CHN$_i$s cluster head of node Nj.

Protocol:

Ni→CHm
PBm{Ni, Ni, Nj, PKi[T, R, M, Hash (M| T| R)]}

CHm→CHn
PBn{CHm, Ni, Nj, PKm[T, R, M, Hash (M| T| R)]}

CHn→Nj
PBj {CHn, Ni, Nj, PKn[T, R, M, Hash (M| T| R)]}

Nj→CHn
PBn{Nj, Ni, Nj, PKj[T, R, M, Hash (M| T||R)]}

CHn→CHm
PBm {CHn, Ni, Nj, PKn[T, R, M, Hash (M| T| R)]}

CHm→Ni
PBi{CHm, Ni, Nj, PKm[T, R, M, Hash (M| T| R)]}

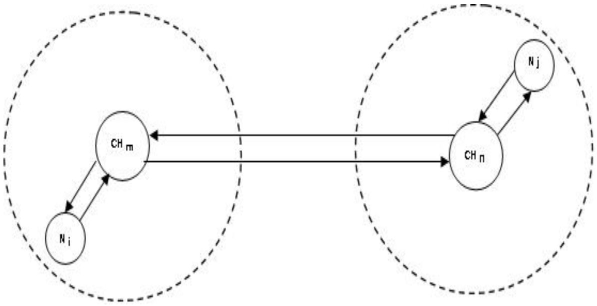

Figure 3: Nodes Ni and Nj belong to different cluster.

IV. SECURITY ANALYSIS

The above protocol achieves the entire security requirement.

A. Authentication:

Authentication of the data transmitted between **Ni** and **Nj** is achieved by using **Sender Identity Final/ Inter** which helps to find the sender of this packet. The **data packet** is decrypted using **Sender Private Key Final/Inter** that authenticates the whole packet is send by the known sender.

B. Confidentiality:

Confidentiality of the data transmitted between Ni and Nj is achieved by encrypted the whole packet by Receiver's public Key Final/Inter. As the packet is encrypted by the Public key no other user expect actual receiver of the packet is able to read the contents of the packet, as the key required to decrypt the packet is private key of the receiver which is known only to the receiver.

C. Integrity:

Integrity of the data transmitted between **Ni** and **Nj** is achieved by including **Hash (M| T| R)** with the original message. When the packet arrives at the receiver node it calculates Hash' **(M| T| R)** and compares Hash' and Hash. If both the Hash equals then packet is accepted otherwise the packet is rejected making the claim on the integrity of the packet.

D. *Non-Repudiation:*

Non-Repudiation of the data transmitted between **Ni** and **Nj** is achieved by encrypted the data packet by the **Sender's Private Key Final/ Inter** of the sender; thus sender can't refuse about not sending the packet. As the user don't know private key of other users no other user can pretend to be other.

V. CONCLUSION AND FUTURE WORK

We have presented a novel protocol to provide cluster based secure communication using public key cryptography technique. Without the fixed infrastructure, provision of security model in mobile ad hoc networks is a challenging task and requires high computation. Proposed protocols require reasonable computational power as compared to other protocol.

Further Clustering protocols in the MANETs can be grouped into six categories according to their objectives: [4]

1. *Dominating-Set-based (DS-based) clustering.*
2. *Low Maintenance Clustering.*
3. *Mobility Aware Clustering.*
4. *Energy Efficient Clustering.*
5. *Load Balancing Clustering.*
6. *Combined metric based Clustering.*

REFERENCES

[1] Varadharajan V, Shankaran R, Hitchens M. Security for cluster based ad hoc networks. Compute Commun, Vol. 27, p. 488–501, 2004.

[2] Jung- San Lee and Chin-Chen Chang, Secure Communications for cluster – based ad hoc networks using node identities, Journal of Network and Computer Applications, Vol.30, pp.1377-1396, 2007

[3] Shuyao Yu, Youkun Zhang, Chuck Song, Kai Chen, "A Security Architechture for Mobile Ad hoc Network" INiEEE International Conference, Dept. of Comput. Sci.2006,

[4]Hengjun Wang, Yadi Wang, Jihong Han, "A Security Architecture for Tactical Mobile Ad Hoc Networks," wkdd, pp.312-315, 2009 Second International Workshop on Knowledge Discovery and Data Mining, 2009

[5] Shaikh, R.A.; Shaikh, Z.A, "A Security Architecture for

Multihop Mobile Ad hoc Networks with Mobile Agents"9th International Multitopic Conference, IEEE INMIC 2005.

[6] Ammayappan, K.; Sastry, V.N.; Negi, A., "Cluster based Multihop Security Protocol in MANET using ECC", TENCON 2008 - 2008 IEEE Region 10 Conference, 19-21 Nov 2008.

[7] Hung-Yu Chien, Ru –Yu Lin Adhoc Networks,Improved ID-basedsecurity framework for adhoc network, Vol.6, pp.47-60, 2007.

[8] HE Yijun, XU Nan and LI Jie A secure key exchange and mutualauthentication protocols for wireless mobile communications,Proceedings of 2nd International conference on Availability, Reliability and Security, pp. 558-563, 2007.

Shrinivas V. Karwa received B.E degree from Sinhgad College of Engineering, Pune in 2008 and currently pursuing M.Tech from Veermata Jijabai Technological Institute, Mumbai. His current research includes Network Security, Cryptography, and Operating system. He did Red Hat Certified Engineer (RHCE) certification.

Vishruti Desai is working as a lecturer in C.K. Pithawala College of Engineering, Surat since last 7 years. She has completed her graduation in B.E. (Computer) from Surat and currently pursuing M.Tech from VJTI, Mumbai. Her current area of interest is computer network, algorithms and wireless sensor networks.

Ashwini Dalvi is working as a lecturer in K.J. Somaiya College of Engineering Mumbai since last 4 years. She has completed her graduation in B.E. (Electronics and Telecommunication) from Mumbai University and currently pursuing M.Tech from VJTI, Mumbai.

Dr. B. B. Meshram is professor and head of computer Technology Department at VJTI, Mumbai. He received bachelor, masters and doctoral Degree in computer Engineering.He has participated in more than 16 refresher courses to meet the needs of current technology. He has chaired more than 10 AICTE STTP programs. He has received the appreciation at Manchester and Cardip University, UK. He has contributed more than 70 research paper at national, International Journal. His current research interest is Databases, Data Warehouse, Web Engineering and Network Security.