Volume 2, No. 2, Mar-Apr 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

A Secure Communication Protocol for Mobile Ad-hoc Networks

Sandeep Kanagala*
SITE, VIT University,
Vellore, India
sandeep.kanagala@gmail.com

Prof. Usha Devi. G
Assistant Professor (Senior Grade)
SITE, VIT University
Vellore, India
ushadevi.g@vit.ac.in

Abstract: **Mobile ad-hoc networks (MANET) is an autonomous collection of mobile users that communicate over bandwidth considered constrained wireless links. They are dynamically reconfigured networks. MANET's face serious security problems with their unique characteristics such as mobility, dynamic topology, and lack of central infrastructure support. Key management is crucial part of security, this issue is even bigger in MANET's. The distribution of encrypted keys is an authenticated manner. Re-keying process will be performed only when a node leaves or joins the network. The communication cost is reduced by re-keying i.e. each cluster will have 1-hop nodes. The cluster heads will be nominated by using lowest id algorithm. The authentication is provided in between communicating nodes. The network lifetime will be extended by using a monitoring node.**

Keywords: **clusters; group-key; network topology; public key; private key; hash value;**

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) allow for the formation of a network without requiring a fixed infrastructure. These networks only require that nodes have interoperable radio hardware and are using the same routing protocol to route traffic over the network. The less requirements for such networks, along with the ability to implement them using small, resource-limited devices has made them increasingly popular in all types of application areas. Since there is no fixed infrastructure, the nodes in the network forward traffic for one another in order to allow communication between nodes that are not within physical radio range. Nodes must also be able to change how they forward data over the network as individual nodes move around and acquire and lose neighbors, i.e., nodes within radio range.

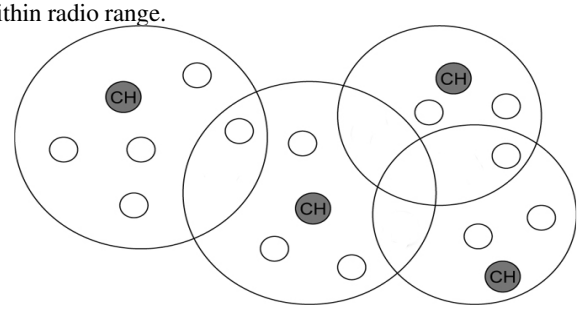

Figure 1. Formation of clusters

This structure has two main advantages: first, it is more robust than existing ones. In fact, each cluster can be seen as a key distribution zone. However key distribution is not achieved by only one node, rather, all the core members have this responsibility. This redundancy strengthens the fault-tolerance of the key distribution scheme within the cluster as the cluster continues to function as long as there is at least a non failing node in the core. Second, as the core members are neighbours, the key agreement protocol used to generate the key of the cluster is low cost and terminates in reasonable delay. This contributes to the rapid deployment of the key in the cluster.

The whole network is divided into clusters and these clusters form a network. Each cluster has a cluster head, and the remaining nodes are cluster nodes or ordinary nodes. Each cluster head maintains the group key and distributes it to remaining nodes within its cluster. Initially each and every node is assigned an id, status code, public key and private key.

Here, security is provided based on re-keying. Re-keying is done by cluster head when any node leaves or joins the network to ensure backward secrecy (a new member should not know the previous information that was exchanged) and forward secrecy (an existing member should node receive any information exchanged after it leaves the network). The encryption and decryption of the data is done by DES algorithm.

Routing protocols are used to determine how to forward the data as well as how to adapt to topology changes resulting from mobility. Initial MANET routing protocols, such as AODV [10], were not designed to withstand malicious nodes within the network or outside attackers nearby with malicious intent. Subsequent protocols and protocol extensions have been proposed [1,2].

Many of these protocols seek to apply cryptographic methods to the existing protocols in order to secure the information in the routing packets. It was quickly discovered, however, that while such an approach does indeed prevent tampering with the routing information, it also makes for a very simple denial of service (DoS) attack [3]. This attack is very effective in MANETs as the devices often have limited battery power in addition to the limited computational power.
It has been suggested that various trust mechanisms could be used to develop new protocols with unique security assurances at different levels. [5,27].

The routing protocol SAODV[6], uses cryptographic methods to secure the routing information. This uses trust metrics to allow for better routing decisions and penalize uncooperative nodes.

II. GROUP KEY GENERATION AND DISTRIBUTION

When a node comes within the radius of the cluster, it sends a hello message with its public key and id. The cluster head receives the message and calculates the group key. The cluster head uses the entire nodes public keys to calculate the group key. It is calculated as follows.

Group-key = $(A)^{p1+p2+\ldots pn+k}{}_{ch}$ mod p * S_{rv}

Where A – primitive root pf p

P1, p2,…pn – public keys of individual nodes within the radius of the cluster,

P – prime number and

S_{rv} – secret random value generated every time while rekeying.

A. *FORWARD AND BACKWARD SECRECY*

Backward secrecy prevents a new member from accessing the communication sent before it joins the group. We remind that in our protocol, a new group member joins a cluster and the key of the cluster is obtained by the combination of the shares of the core members. Furthermore, the key of the cluster is encrypted with the KEK generated by every core member using the shares of all the periphery members that are attached to it. So, an adversary needs to find all the shares of the core members or all the shares of the periphery members that are attached to a given core member. This property makes it impossible for the adversary to compute a previous cluster key. Furthermore, since the secret of the concerned core member and the secret of the cluster head are changed after each join operation, it is impossible for a new member or an adversary to find these secrets from the keys it has received at join. Forward secrecy prevents an old member from accessing current communication after it leaves the group. In our protocol, it is impossible for an adversary to compute the current group key after its leaves for the same reason we mentioned about the backward secrecy. Even having the public values of all members' secrets, the adversary cannot compute the current cluster key [11, 12].

III. NEW NODE JOINS

When node X joins in the cluster, it sends a hello message, id, and its public key to the cluster head. The cluster head calculates the group key and distributes it to other nodes. The cluster head unicasts it to the node X. The group key will be encrypted using a new node public key.

CH -> new node: Enc(Pubnode, (Enc(e,[K_0])||(d,n)))

Where Pubnode – public key of new node

IV. EXISTING NODE LEAVES

When an existing node Y leaves the cluster, it sends a leave message, with its id to the cluster head. The cluster head calculates the new group key and multicasts the group key to other nodes.

CH -> all node: Enc(Pubnode,(Enc(e,[k_0])||(d,n)))

Where Pubnode – public key of existing node.

V. PROVIDING SECURITY

A. *Within the network if any two nodes want to communicate first they will authenticate each other and the steps are as follows.*

- Node X calculates hash value using its id, public key, and group key and transmits the hash value, id and public key to other node Y.
- Node Y receive hash value and also it calculates new hash value from node X's id, public key and group key.
- Node Y will check the received values and calculated value both are equal or not.
- If the hashed values are equal, it identifies the peer node as authenticated node.

VI. RESULT

So, we consider the above routing protocol to calculate the communication cost and transmission delay.

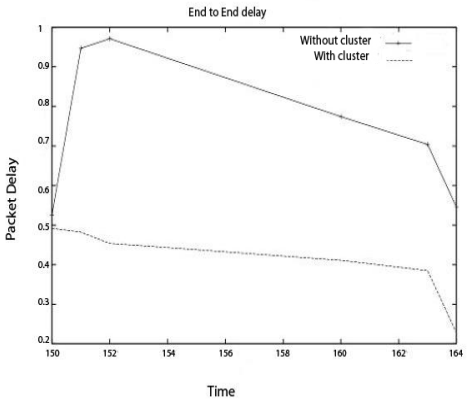

Figure 2. Graph showing transmission delay

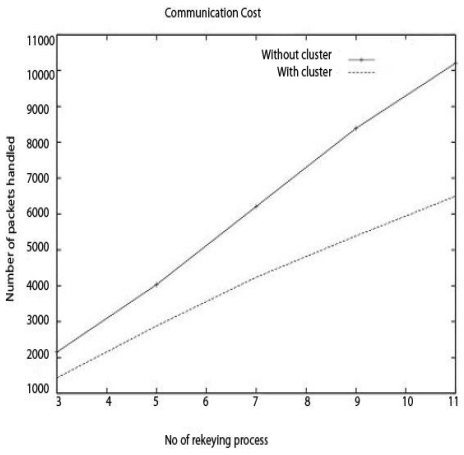

Figure 3. Graph showing communication cost

From fig 2 we can say that transmission delay is less when packets are transferred without clusters. By considering fig 3

we can say that communication cost of packets is less when packets are transferred without clusters.

VII. CONCLUSION

Several protocols for wireless ad-hoc networks have been proposed. No protocol is accepted as standard because every protocol has advantages and disadvantages over each other. So, from fig 2 and fig 3 we can say that the comparison of communication cost and transmission delay are more when no clusters are used.

VIII. REFERENCES

[1] C. N.-R. Baruch Awerbuch, David Holmer and H. Rubens. An on-demand secure routing protocol resilient to byzantine failures. In ACM Workshop on Wireless Security (WiSe), September 2002.

[2] S. Buchegger and J.-Y. L. Boudec. Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks. In Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing. IEEE Computer Society, January 2002.

[3] M. Jakobsson, S. Wetzel, and B. Yener. Stealth attacks on ad hoc wireless networks. In Proceedings of VTC, 2003, 2003.

[4] L. Eschenauer, V. Gligor, and J. Baras. On trust establishment in mobile ad-hoc networks. Technical Report MS 2002-10, Institute for Systems Research, University of Maryland, MD, USA, October 2002.

[5] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas. A quantitative trust establishment framework for reliable data packet delivery in manets. In SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, pages 1–10, New York, NY, USA, 2005. ACM Press.

[6] M. G. Zapata and N. Asokan. Securing ad hoc routing protocols. In WiSE '02: Proceedings of the ACM workshop on Wireless security. ACM Press, 2002.

[7] K. Meka, M. Virendra, and S. Upadhyaya. Trust based routing decisions in mobile ad-hoc networks. In Proceedings of the Workshop on Secure Knowledge Management (SKM 2006), 2006.

[8] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. In Imielinski and Korth, editors, Mobile Computing, volume 353. Kluwer Academic Publishers, 1996.

[9] Huston, Kevin R; Schlosser Terri L.; Shier, Douglas R. On the Distributes Bellaman-Ford Algorithm and the Looping Problem. Informs Journal on computing. September 22, 2007.

[10] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on-demand distance vector (aodv) routing. July 2003.

[11] D. Augot, R. Bhaskar, V. Issarny, D. Sacchetti, A three round authenticated group key agreement protocol for ad hoc networks, Pervasive and Mobile Computing 3 (1) (2007) 36–52.

[12] D. Boneh, The decision Diffie–Hellman problem, in: ANTS-III: 3rd Algorithmic Number Theory Symposium, ANTS-III, in: LNCS, vol. 1423, 1998, pp. 48–63.