ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 7 (July 2013), Page No. 2262-2265

A Trusted-Group Criteria for Performing Trust Aware Routing in Mobile Networks

Beenu Shokeen[1] , Rashmi[2]

[1]Computer Science and Engineering Department, PDM College of Engineering, Bahadurgarh, Haryana
bnshokeen2@gmail.com

[2]Assisstant Professor of Information Technology, PDM College of Engineering, Bahadurgarh , 124507, Haryana
rashmi.31130@gmail.com

Abstract : ***Security is a significant issue in Wireless Mobile Networks. Intrusion of malicious nodes may cause serious impairment to the security. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. A Mobile network is one of the most widely open network in which any intruder or the selfish node can easily perform an attack and affect the communication reliability. The presented work is about to define an effective and trustful communication approach over the network. . In this approach, a group management approach is defined. Each group will be managed by the base station itself. The group authentication will be done based on Diffie-Hellman algorithm***

Key-words: Group Adaptability, Group Key Authentication, Route Generation.

I INTRODUCTION

Ad-hoc networks consist of many mobile hosts connected by wireless links. Each mobile node (MN) operates not only as an end-system, but also as a router to forward packets over the multihop ad-hoc networks. The ad-hoc network topology is dynamic one, so it may change frequently due to the nodes' movements. Routing protocols for ad-hoc networks can generally be divided into two categories. One is a proactive routing protocol that attempts to allow each MN using it to always maintain an up-to-date route to each possible destination MN in the mobile wireless network. Other is on-demand routing protocol to establish routing path when a specific MN wants to send data to destination MN [1, 2, 3, 4]. The basic concept of these protocols is flooding that overwhelming amount of packet trfansmission, most of them unnecessary, can quickly exhaust the battery of hosts and may hang up the entire network as a result of severe packet contention and collision [5, 6, 7].

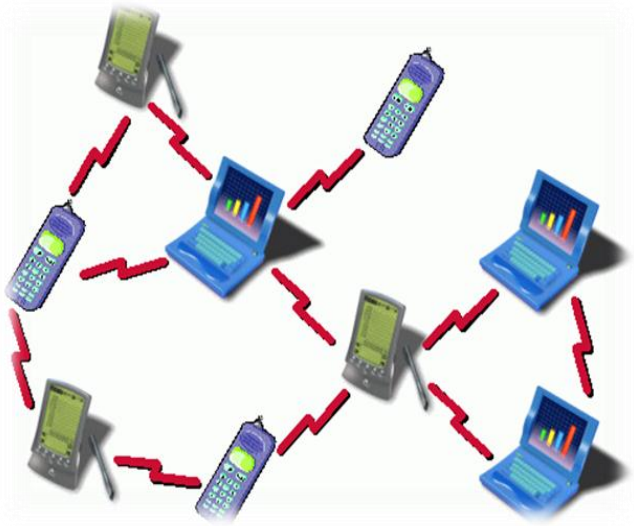

Figure1: Mobile Ad-hoc Network

1.1 MANET

A MANET (Mobile AdHoc Network) is an autonomous collection of mobile users that offers infrastructure-free communication over a shared wireless medium. It is formed spontaneously without any preplanning. Multicasting is a

fundamental communication paradigm for group-oriented communications such as video conferencing, discussion forums, frequent stock updates, video on demand (VoD), pay per view programs, and advertising. The combination of an ad hoc environment with multicast services [1, 2, 3] introduces new challenges towards the security infrastructure. In order to secure multicast communication, security services such as authentication, data integrity, access control and group confidentiality are required[4]. Among which group confidentiality is the most important service for several applications.

A critical problem with any rekey technique is scalability. The rekey process should be done after each membership change, and if the membership changes are frequent, key management will require a large number of key exchanges per unit time in order to maintain both forward and backward secrecies. The number of TEK update messages in the case of frequent join and leave operations induces "1 affects n" phenomenon. To overcome this problem, several approaches propose a multicast group clustering [9, 10, 11,12]. Clustering is dividing the multicast group into several sub-groups. An entity called Local controller (LC) manages each subgroup, which is responsible for local key management within the cluster. Thus, after Join or Leave procedures, only members 2009 International Conference on Advances in Recent Technologies in Communication and Computing within the concerned cluster are affected by rekeying process, and the local membership dynamism within a cluster does not affect the other clusters of the group.

This paper proposes an EOMCT (Enhanced Optimized Multicast Cluster Tree) algorithm for efficient multicast key distribution in mobile adhoc networks.

1.2 Multicast Routing Algorithm For Ad-Hoc Network

The Prior to create a multicast routing tree in ad-hoc network, this paper generates basic trees that all MNs broadcast request packet (REQ) to BN and they receive reply packet (REP) from BN or upper MN with logical address including location field. After establishing its basic tree, when the source MN-a wants to join a specific Mcast group, at first, the MN-a investigates its mapping table to identify MNs on its basic tree and its NMNs on other basic trees whether they manage the Mcast group or not. If the table of MN-a contains Mcast group, then the Mcast path will be established via its basic tree or NMNs. Otherwise, MN-a broadcasts JOIN packet for Mcast group to its tree and NMNs. Upper and lower MNs on the basic tree and its NMNs which received JOIN packet examine their mapping table. If any table has Mcast group MNs on basic tree or NMNs, simply it joins the Mcast group through them, otherwise only MNs on its tree broadcast Mcast JOIN packet also, and NMNs check only their table manage Mcast group or not. In this case MN-a may receive some routing information from MNs on its basic tree and their NMNs, then MN-a selects an ondemand Mcast routing path with minimum hop count. Otherwise, the JOIN packet to Mcast group is arrived BN, then BN supports a path using MN-a's basic tree and another basic tree which control Mcast group. Note that although all the NMNs which controlled by other trees receive Mcast JOIN packet from a specific tree they do not broadcast JOIN packet at any case but investigate only whether they have a table for a specific Mcast group or not.

The procedure for creating overlay Mcast routing tree explained above is summarized as follows,

i) Source MN-a broadcasts JOIN packet with Mcast group address

ii) All MNs received Mcast JOIN packet examine their mapping table whether they have MNs that already joined Mcast group or not.

iii) If any MN has joined Mcast group, then it sends ACK with hop-count toward source MN else it discards Mcast JOIN packet excluding upper and lower MNs on MN-a' basic tree and go to step (v)

iv) If MN-a checks hop-counts towards Mcast-source MN via NMN and appropriates them, then NMN sends Mcast packet to MN-a else MN-a sends DN(deny) packet to that NMN and goto step (vi)

v) MN-a receives Mcast group packet via NMN when transmission is complete

vi) Upper and lower MNs on MN-a's basic tree broadcast Mcast JOIN packet until arrive it to BN, and if any MN on its basic tree identifies no path via its tree, then the BN sends ACK packet to MN-a with joinable basic tree via BN

vii) MN-a receives Mcast group packet via BN

viii) MN-a prunes Mcast group when transmission is complete.

The method for generating on-demand Mcast tree using broadcasting JOIN packet from source MN and other MNs within its basic tree.

1.3 Manets Routing Protocols

Mobile Ad-Hoc Network is the rapid growing technology from the past 20 years. The gain in their popularity is because of the ease of deployment, infrastructure less and their dynamic nature. MANETs created a new set of demands to be implemented and to provide efficient better end-to-end communication. MANETs works on TCP/IP structure to provide the means of communication between communicating work stations. Work stations are mobile and they have limited resources, therefore the traditional TCP/IP model needs to be refurbished or modified, in order to compensate the MANETs mobility to provide efficient functionality. Therefore the key research area for the researchers is routing in any network.

Routing protocols in MANETs are classified into three different categories according to their functionality.

1.Reactive protocols
2.Proactive protocols
3.Hybrid protocols

II ISSUES WITH EXISTING WORK

- In the existing work, no initial eligibility group membership criteria is defined for a node But in this presented work, we have defined an eligibility criteria based on response time, mobility vector and throughput analysis.
- In existing work, a symmetric criteria is defined for next hop selection in all cases. But in this proposed work, we have defined two different criteria. One, for the node within group and second for intergroup communication.
- A weighted approach will be implemented to identify trustfulness of the nodes.

III OBJECTIVES

- The main objective of the work is to define a group key authentication over the mobile groups based on which the trust level of each node will be defined.
- We will define a new parametric consideration of trustworthy next hop selection based on node existence in same group and in other group.
- The overall objective of the work is to define a trustful route over the network that will give effective communication in case of selfish nodes as well as in congested networks.
- The anlaysis will be driven in terms of nodes trustworthiness and the network throughput.

IV PROPOSED WORK

The proposed work is the improvement over a trust aware routing over the network by performing a group key authentication along with trustworthy next hop selection over the network. The complete work is divided in three sub tasks:

- **Group Adaptability**
  In this work, a node will be verified to be the part of a specific group or not. The group validity will be checked under some defined constraints. In this work we have defined three main constraints

(i) Communication Range
(ii) Throughput Analysis
(iii) Response Time

The communication range is basically defined as the coverage area in terms of neighbour node selection. The communication range will selected based on the direct one to one communication basis. Based on the same parameter the transmission rate will be analyzed along with response time. A node that will provide effective and efficient throughput in defined time will be elected as the group member.

- **Group Key Authentication**

At the second phase the authentication scheme is defined under the diffie-hellman based group key approach to identify the validity of node. We have used group key based crypto analysis for the session management. Each node of the group will be assigned by same public key that will be verified by a group manager or the base station. The authentication will be maintained only once as the communication will begin and the session will be established. Once the session declared the route generation will be performed.

- **Route Generation**

The motive of the work is to generate a trust aware route over the network. The trustfulness of a node will be defined separately based on the route existence in a group or outside the group. If the next hop exist in the group itself, the trust level will be analyzed by using two main parameters called

(i) Response Time Analysis
(ii) Membership time in a group

If the node does not exist in same group the parameter depends on three main parameters

(i) Response Time
(ii) Membership time in a group
(iii) Number of Overlapping Groups

Authentication Phase

First test is performed for the authentication of a node. A node encrypts its data with the shared secret key (g)ab which is calculated by two nodes previously; and transmits it the route. This key is known to only these two nodes who are actually communicating. At receiver's end the data will be decrypted by applying the inverse of (g)-ab. If a node replies back within a time period then it is assumed to be an authentic node. If its response time exceeds current time-request time; it will be considered as a compromised node. If it's a compromised node then find all the compromised node of i and the same process is repeated again for the remaining nodes to find the next authentic node of the network. This is the first level of trust.

Algorithm

Algo(S,D)
/*S is the source Node and D is the Destination Node*/
{

1. Find the path between S and D called P1,P2,P3….Pn
2. For Each Node Generate the KeyGroup for the communication using Deffie-Hellman Algorithm
   a. Unique Priavate Key Pvk
   b. Global Public Key Puk
   c. Shared Key Shk
3. On Node S Retrive the Public Key of D and Perform the encryption

4. Perform the Communication between Source and Destination

5. For Each Node in path called Pi verify the shared key

6. On Reciever Side Perform the Decoding using PrivateKey(D)

7. Discard the Bad Packets coming from unauthorized nodes.

8. Perform the Secure Communication over the network.

}

V CONCLUSION

The objectives listed have been carried out. In the presented work, we have discussed about wireless mobile network and its architecture. Additionally it includes a review of different threats associated with networks and their defensive measures. Then routing in wireless sensor networks was discussed. As most of the routing protocols are not designed taking security issues into account, most of them are prone to different types of attacks. Even some of the protocols are vulnerable to those attacks. Most of the routing protocols used cryptographic techniques such as public key cryptosystem: RSA, Hashing etc. to secure the data transmission and the transmission link from different types of attacks.
In this work, a group key based authentication scheme is defined to perform the reliable communication over the network. The reliability of a node can be identified by analyzing its membership factor to a group. A group member is more reliable as compared to other node. The group member ship is the major phenomenon discussed in this work. The authentication and some other parameters are defined to prove the group eligibility of a node.

VI FUTURE WORK

The presented work is defined to provide a secure and reliable communication in a mobile network. To achieve this, group based authentication and reliable approach is defined. The diffie-hellman approach is here used for the authentication. The presented work can be extended in different ways in future.

- Instead of using the Diffie-hellman algorithm more secure and authenticated ways can be used for the group verification.

- The work can also tried on a clustered network.

VII REFERENCES

[1] Sung-Ju Lee, William Su, Julian Hsu, Mario Gerla, and Rajive Bagrodia," A Performance Comparison Study of Ad Hoc Wireless Multicast Protocols", IEEE 2000.

[2] C-K. Toh," Performance Evaluation of Flooding-Based and Associativity-Based Ad Hoc Mobile Multicast Routing Protocols", IEEE 2000.

[3] I.Chatzigiannakis, S.Nikoletseas and P.Spirakis, "An Efficient Routing Protocol for Hierarchical Ad-hoc Mobile Networks", IEEE 2001.

[4] Chae Young Lee and Hee Kwun Cho, "Multicast Routing Considering Reliability And Network Load In Wireless Ad- Hoc Network", IEEE 2001

[5] S.Radha, S.Shanmugave, L.Hemalatha, S.Kavitha, T.Lakshmi, "Performance Evaluation of Multicasting in MANET Using Node Transition Probability Based Routing Algorithm", IEEE 2002.

[6] Pedro M. Rniz', Graeme Brown', Ian Groves, "Scalable multicast communications for ad hoc extension attached to IP Mobile Networks", IEEE 2002

[7] G. Chelius, E. Fleury, F Valois, "Adaptive and Robust Adhoc Multicast Structure", IEEE 2003.

[8] J. Ye, W.C. Wong and K.C. Chua, "Power-Efficient Multicasting in Ad Hoc Networks" , IEEE 2003

[9] Steffen Blodt, " Efficient End System Multicast for Mobile Ad Hoc Networks", IEEE 2004.

[10] J. Ye and K.C. Chua &W.C. Wong," Power Conservation and Path Efficiency for MulticastAdHocNetworks",IEEE2004.

[11] K. Daniel Wong, T.J. Kwon, V. Varma, " Towards Commercialization of Ad Hoc Networks", IEEE 2004.

[12] Larry Hughes, Atekeh Maghsoudlou, "An Efficient Coverage-based Flooding Scheme for Geocasting in Mobile Ad hoc Networks", IEEE 2006.