A Novel Support for Secure Neighbor Sighting and Authentication in Mobile Ad-Hoc Network (MANET)

[1]Gobinath. C
[2]Karthik. G
[1]Assistant Professor, Department of Information Technology
[2]Assistant Professor, Department of Information Technology
Kongunadu College of Engineering and Technology,
Trichy, Anna University

***Abstract*:- An ad hoc mobile network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. In Mobile Ad-Hoc Networks, routes may be disconnected due to dynamic movement of nodes. Such networks are more vulnerable to both internal and external attacks due to presence of adversarial nodes. These nodes affect the performance of routing protocol in Ad-Hoc networks. So, it is essential to identify the neighbors in a MANET. Neighborhood discovery (ND) is the process of discovering the devices that are directly reachable for communication or in physical proximity. It becomes a fundamental requirement and building block for various other applications. It is easy to abuse ND and thereby compromise the overlying protocols and applications. Thus, providing methods to mitigate this vulnerability and secure ND is crucial. The proposed scheme identifies neighbors and verifies its position effectively by using SNDA protocol and transferring the data packet at secure manner.**

Keywords: Snda, Manet, Nd, Slv

I. INTRODUCTION

An ad hoc network is a collection of nodes that do not need to rely on a predefined infrastructure to keep the network connected. Ad hoc networks can be formed, merged together or partitioned into separate networks on the fly, without necessarily relying on a fixed infrastructure to manage the operation. Nodes of ad hoc networks are often mobile, which also implicates that they apply wireless communication to maintain the connectivity, in which case the networks are called as mobile ad hoc networks (MANET). Mobility is not, however, a requirement for nodes in ad hoc networks, in ad hoc networks there may exist static and wired nodes, which may make use of services offered by fixed infrastructure. The most important requirement of the ad-hoc networks is that they are "self-configuring" i.e., that a large number of wireless nodes organize themselves to efficiently perform the tasks required by the application after they have been deployed.

After nodes are deployed, they do not have knowledge about the neighbors thus, they need to discover their neighbors in order to communicate with them. Knowledge of the neighbors is essential for almost all routing protocols, medium-access control protocols and several other topology-control algorithms. Neighbor discovery is, therefore, a crucial first step in the process of self-organization of a wireless ad-hoc network. Neighbor discovery is the process by which a node in a network determines the total number and identity of other nodes in its vicinity. It is a fundamental building block of many protocols including localization [4], routing [8], leader election [12], and group management [5]. Time-based communications and many media access control mechanisms [13] rely on accurate neighbor information. Neighbor discovery is especially important to the proper functioning of wireless networks.

The neighbors can be either physical neighbors or communication neighbor [9]. The physical neighbors are those that are in the range of physical proximity of the discoverer. The

communication neighbors are those that are reachable for communication but need not to be in the physical range of the discoverer.

To address the aforementioned challenges, this paper presents a Secure Neighbor Discovery and Authentication (SNDA) protocol, which allows neighbors to verify that they are speaking directly with each other. Secure Neighbor Discovery and Authentication (SNDA) protocol has the following features.

- It is designed for spontaneous ad hoc environments, and it does not depend on the presence of a trusted infrastructure or of a priori trustworthy nodes.
- It gears the node to perform all verification procedures autonomously.
- It is reactive, (i.e.) it can be executed by any node, at any point in time, without prior knowledge of the neighborhood.
- It is tough against independent and colluding adversaries.
- It is lightweight protocol, and it generates low overhead traffic.

II. RELATED WORK

Secure neighbor discovery (SND) covers a range of techniques and technologies. A variety of approaches have been proposed to handle SND in general and adversaries in particular. Many approaches leverage physical properties of communications and can be roughly divided into solutions based on location, time, time and location, and network geometry. Other solutions rely on security properties achievable in specific scenarios. In [9], Papadimitratos, et al.

give an overview of the problems and challenges associated with SND. Their paper includes a set of real-world examples illustrating various threats to neighbor discovery. Secure neighbor discovery (SND), that is, the discovery of directly reachable nodes (communicating neighbors) or nodes within a distance (physical neighbors) [9]. To put it simply, an adversarial node could be securely discovered as neighbor and be indeed a neighbor (within some SND range), but it could still cheat about its position within the same range. SND is a subset of the SNPD problem, since it lets a node assess whether another node is an actual neighbor but it does not verify the location it claims to be at. Nonetheless, properties of SND protocols with proven secure solutions [6], [7], are useful in our context: as an example, signal Time of Flight based and other distance measurements between two nodes can prevent relay attacks (i.e., malicious nodes relaying, stealthily and verbatim, messages of other correct nodes).

Johnson and Maltz [2,3] point out that conventional routing protocols are insufficient for ad hoc networks, since the amount of routing related traffic may waste a large portion of the wireless bandwidth, especially for protocols that use periodic updates of routing tables. They proposed using Dynamic Source Routing (DSR), which is based on on-demand route discovery. A number of protocol optimizations are also proposed to reduce the route discovery overhead. Perkins and Royer [1] present the AODV (Ad hoc On demand Distance Vector routing) protocol that also uses a demand-driven route establishment procedure.

Neighbor position verification was investigated in the context of ad-hoc networks, with solutions relying on dedicated mobile or hidden base stations [11], or on the availability of a number of trustworthy devices [10]. Our SNDA protocol, instead, is a fully distributed solution that does not require the presence of any particular infrastructure or a-priori trusted neighbors. Also, unlike previous works, our solution targets highly mobile environments and it assumes the initiator node changes according to energy level.

III. PROPOSED METHODOLOGY

This paper explores the possibility of using location information to improve performance of routing protocols for MANET. SNDA protocol is used to exchange the messages and verifies the position of communicating nodes. In this Protocol, four set of messages are exchanged. They are:

a. SURVEY message

b. RESPOND message

c. DISCLOSE message

d. DETAILS message

SURVEY message - An initiator I initiates this message. This message is anonymous. The verifier identity is kept hidden.

RESPOND message - A communication neighbor N receiving the SURVEY message will broadcast RESPOND message after a time interval. This also internally saves the transmission time.

DISCLOSE message - The DISCLOSE message broadcasting is done by using Initiators real address. It contains a map MP, a proof that I is the author of the original SURVEY message and the verifier identity,

DETAILS message - The DETAILS carries N's position, the transmission time of N's RESPOND, and the list of pairs of reception times and temporary identifiers referring to the RESPOND broadcasts N received. The identifiers are obtained from the map MP included in the DISCLOSE message.

1. Secure Neighbor Discovery

The Secure Neighbor Discovery and Authentication (SNDA) protocol is a security extension of the Neighbor Discovery Protocol (NDP). The proposed protocol works within a given distance, then the nodes are identified and recognize the

communication links also. It is susceptible to malicious interference and hence considered to be not secure node. SNDA provide an alternate mechanism for securing NDP with a cryptographic method. The Neighbor Discovery Protocol (NDP) is responsible in for discovery of other network nodes on the local link, and to find available routers, and maintain reachability information about the paths to other active neighbor nodes. In proposed approach every neighbor node can use the SNDA protocol so the initiator node process will be handled by any neighbor nodes. The interchanging procedure of the initiator node improves the total network security and it protects the network from the more number of malicious nodes.

2. Position Verification

To verify the position of a node following three tests is done, they are

- Direct symmetry test
- Cross symmetry test
- The Multilateration Test.

In the Direct Symmetry Test (DST), I verifies the direct links with its communication neighbors. To this end, it checks whether reciprocal Time of Flight-derived distances are consistent with each other, with the position advertised by the neighbor, and with a proximity range R. In cross symmetry test, information mutually gathered by each pair of communication neighbors are checked. This ignores nodes already declared as faulty by the DST and only considers nodes that proved to be communication neighbors between each other, i.e., for which To D-derived mutual distances are available. In multilateration test, the unnotified links are tested. Once all couples of nodes have been checked, each node N for which two or more unnotified links exists is considered as suspect.

Location verification allows nodes to have condensed in the location of their neighbors, preventing many basic attacks on routing. In routing, many possible attacks are performed. Without verification, a malicious node can fake its location information. The Secure Location Verification (SLV) has the capability of detecting position spoofing attacks. SLV is an infrastructure-less cooperative scheme.

The communication link is established within the distance, and identifying the nodes location is termed as Neighbor Discovery. An adversarial node could be securely discovered as neighbor and be certainly a neighbor within some range, but it could still cheat about its position within the same range. In other words, SND lets a node assess whether another node is an actual neighbor but it does not verify the location it claims to be at this is most often employed to counter adversaries attacks. An ad hoc network is a collection of wireless mobile hosts forming a temporary network without the help of any conventional

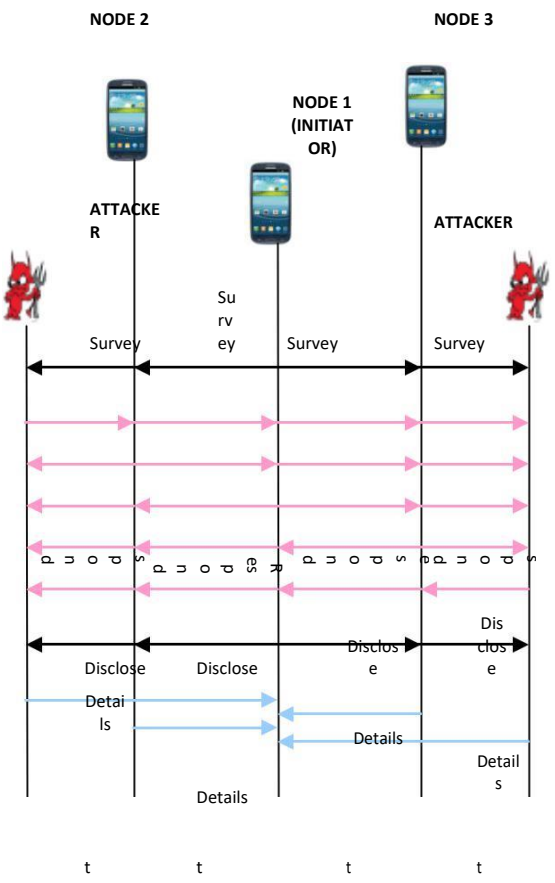
infrastructure or centralized administration. In such an environment, it is necessary for one mobile host to enroll the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. In order to obtain the position of other nodes while moving, an approach is proposed such a way that it helps to obtain the position of a dynamic mobile node.

3. System Model

A set of mobile terminals forms a spontaneous ad hoc network. It is a lightweight protocol and it is special cases of ad hoc network, in which the mobile terminals are connected with each other, share the resources, services during a limited time of period and limited space. A well defined, efficient and user friendly security mechanisms are required for spontaneous ad hoc networks. Spontaneous networks can be wired or wireless. Here it considers the wireless spontaneous networks. Their objective is the integration of services and devices in the same environment enabling the user to have instant service without any external infrastructure. Spontaneous networks are special case of human centric networks. A user without advanced technical knowledge can set up and participate in a spontaneous network. Spontaneous ad hoc networks require well defined, efficient and user-friendly security mechanisms. The security schemes will allow secure communication between end users. The different tasks to be carried out in these ad hoc networks are address assignment, user identification, user authorization, name service and their safety. Infrastructure wireless networks use Certificate Authority (CA) servers to manage node authentication and trust. Its computing capacity should be higher in rate. Security is based on anonymity, confidentiality, node cooperation and privacy.

4. Data Packet Transformation

In the network every neighbor node can use the SNDA protocol so the initiator node process will be handled by any neighbor nodes. Also the data packet transmissions are carried out by selecting and sending through authorized high energy level nodes only this process helps to effective data packet transmission in faster and secure way. The interchanging procedure of the initiator node improves the total network security and it protects the network from the more number of malicious nodes.



ARCHITECTURE DIAGRAM

IV. RESULTS AND DISCUSSIONS

A single independent adversary cannot perform any successful attack against the SNDA protocol. When the shared neighbor-hood increases in size, the probability that the adversary is tagged as faulty rapidly grows to 1. Multiple independent adversaries can only harm each other, thus reducing their probability of successfully announcing a fake position. In coordinated attacks, it is the nature of the neighbor hood that determines the performance of the SNDA scheme in presence of colluders. However, in realistic environments, our solution is very robust even to attacks launched by large groups of knowledgeable colluders. This system yields small advantage to the adversaries in terms of displacement. Finally, the overhead introduced by the SNDA protocol is reasonable, as it does not exceed a few tens of Kbytes even in the most critical conditions.

Graphical Representations

Figure 2 illustrates below, the comparison between existing protocol (NPV) and proposed protocol (SNDA). The comparison graph describes that the proposed protocol giving more security than the NPV protocol.

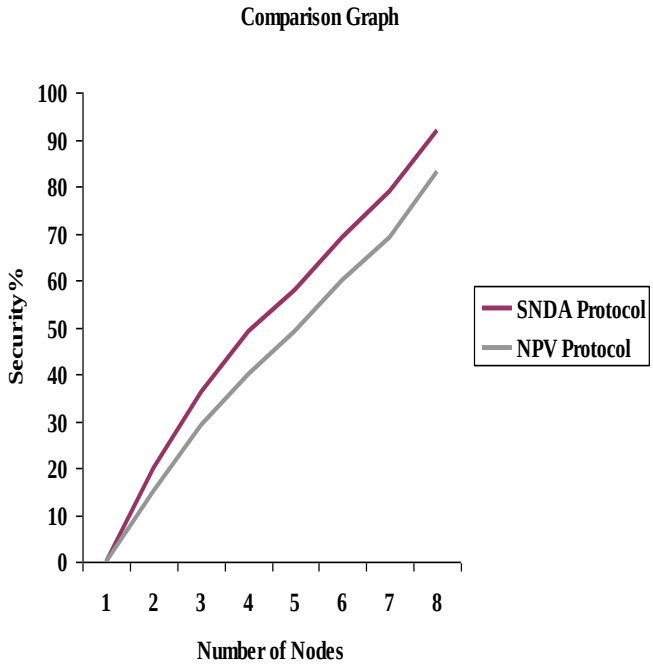


Figure 2: Comparison between NPV vs SNDA

Figure 3 illustrates the data packet delivery ratio. From the figure the paper can conclude that by using the proposed protocol (SNDA) can improve packet delivery ratio, moreover it gives the accuracy of transmission path also.

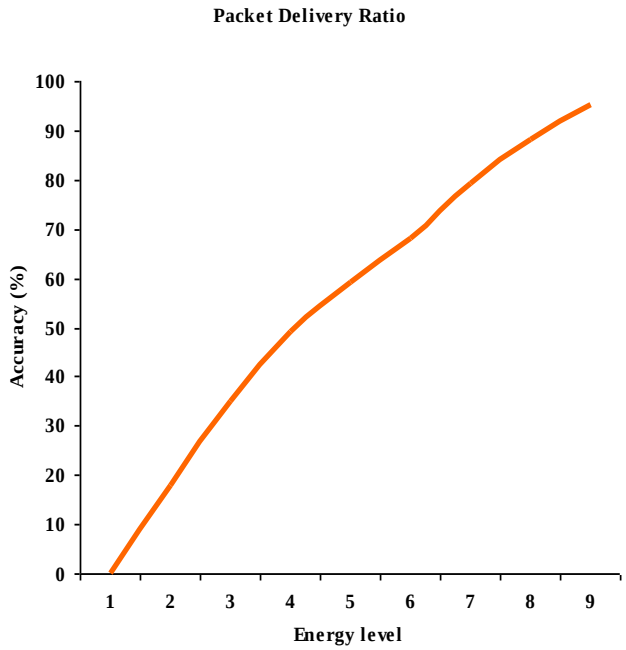


Figure 3: Packet delivery ratio

V. CONCLUSION

The SNDA techniques will ultimately provide security from malicious nodes. The protocol is robust to adversarial attacks. A brief study of discovery and verifications of neighbor position is given in this paper. Security analysis was enhanced by integrating the SNDA protocol with secure MANET protocol. As a future work, improve more security by using finest cryptographic method.

REFERENCES

[1] C.E. Perkins and E.M. Royer, Ad hoc on demand distance vector (AODV) routing (Internet-draft), in: Mobile Ad-hoc Network (MANET) Working Group, IETF (1998).
[2] D.B. Johnson and D.A. Maltz, Dynamic Source Routing in Ad Hoc Wireless Networks (Kluwer Academic, 1996).
[3] D. Johnson, D.A. Maltz and J. Broch, The dynamic source routing protocol for mobile ad hoc networks (Internet-draft), in: Mobile Adhoc Network (MANET) Working Group, IETF (1998).
[4] J. Hwang, T. He, and Y. Kim, "Secure localization with phantom node detection," Ad Hoc Networks, vol. 6, no. 7, pp. 1031 – 1050, 2008
[5] J. Liu, D. Sacchetti, F. Sailhan, and V. Issarny, "Group management for mobile ad hoc networks: design, implementation and experiment," in International Conference on Mobile Data Management (MDM), 2005
[6] M. Poturalski, P. Papadimitratos, J-P. Hubaux, "Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility," ASIACCS, 2008.
[7] M Poturalksi, P. Papadimitratos, J.-P. Hubaux, "Towards Provable Secure Neighbor Discovery in Wireless Networks," Workshop on Formal Methods in Security Engineering, 2008
[8] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), 2002. ems (SenSys), 2003
[9] P. P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P Hubaux, "Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networking," IEEE Communications Magazine, vol. 46, no. 2, 2008.
[10] S. ˇCapkun, J.-P. Hubaux, "Secure Positioning in Wireless Networks," IEEE JSAC, 2006.
[11] S. Capkun, K. Rasmussen, M. Cagalj, M. Srivastava, "Secure Location Verification with Hidden and Mobile Base Stations,"IEEE Trans. on Mobile Comp., 2008
[12] S. Vasudevan, J. Kurose, and D. Towsley, "Design and analysis of a leader election algorithm for mobile ad hoc networks," IEEE Conference on Network Protocols (ICNP), 2004
[13] T. van Dam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," in ACM Conference on Embedded Networked Sensor Syst