Volume 3, Issue 10, October 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Study on Secure Spontaneous Ad Hoc Network Protocol for Neighbor Position Verification

Padmavathi K, Jaganraj L
PG Scholar, Department of Computer Science and Engineering,
Kalaignar Karunanidhi Institute of Technology, Coimbatore, TamilNadu, India.

Abstract*— Location awareness is an important asset in mobile systems and many protocols require knowledge of position of the participating nodes. A secure protocol for spontaneous wireless ad hoc networks is used by the hybrid symmetric and asymmetric schemes. It gives the trust between end users for exchanging the initial data. The data can be encrypted by using a secret key which hides the data. First visual contact between users is the main basis for trust. Using the complete self-configured secure protocol, it is being able to create the network and it also shares the secure services without any infrastructure. The network allows resource sharing and offers new services among users in a secure environment. Providing this protocol to a wireless ad hoc network makes it to be more secure. Our proposal is that, by integrating the Neighbor Position Verification protocol with spontaneous ad hoc network protocol, each node in the network can constantly verify the position of its neighbors as well as security analysis of the system.

Keywords*— Neighbor Position Verification protocol, Mobile ad hoc networks, Spontaneous network, Secure protocol.

I. INTRODUCTION

Ad hoc networks are wireless networks with no fixed infrastructure in which nodes depend on each other to keep the network connected. A mobile ad hoc network (**MANET**) is a self-configuring infrastructure-less network of mobile devices connected by wireless. It consists of a collection of mobile hosts that may communicate with each another from time to time. No base stations are supported. In Mobile Ad-Hoc Networks, Routes may be disconnected due to dynamic movement of nodes. Due to mobility in MANETs, each device is free to move independently in any direction, and will therefore change its links to other devices frequently. Each device must forward traffic distinct to its own use, and therefore be a router. The primary challenge in construction of a MANET is equipping each device to continuously maintain the information required to properly direct the traffic. Most traditional mobile ad hoc network routing protocols were designed focusing on the efficiency and performance of the network.

A. Location awareness

Location awareness is becoming an important capability for mobile computing devices, where many protocols need knowledge of the position of the participating nodes. For example, knowledge about neighboring nodes can be used to route, cluster and broadcast in an efficient manner. Whenever a node needs to send data to another node on a network, it must first know where to send it. If the node cannot directly connect to the destination node, it has to send it via other nodes along a proper route to the destination node. Geographic routing in spontaneous networks, data gathering in sensor networks, movement coordination among autonomous robotic nodes, location-specific services for handheld devices, and danger warning or traffic monitoring in vehicular networks are all examples of services that build on the availability of neighbor position information. Here, the challenge is to perform, in absence of priori trusted nodes, a fully distributed, lightweight NPV procedure that enables each node to attain the locations advertised by its neighbors, and evaluate their truthfulness.

An NPV 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.

B. Npv protocol

NPV 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:

- POLL message
- REPLY message
- REVEAL message
- REPORT message

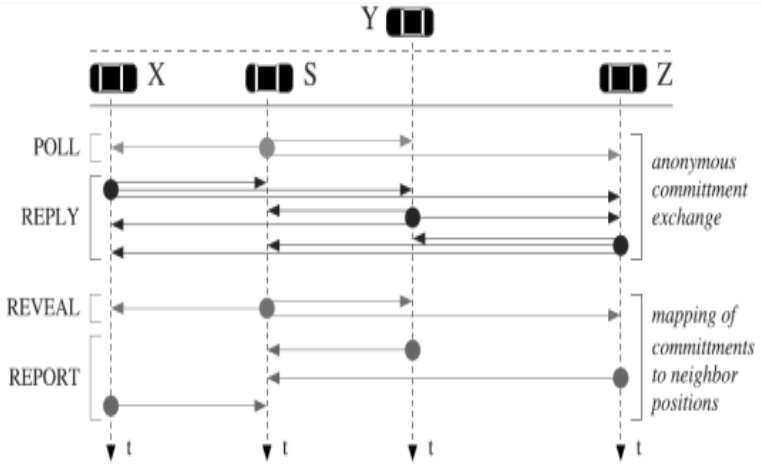

Fig 1: Message exchange

- *POLL message*

A verifier S initiates this message. This message is anonymous. The verifier identity is kept hidden. Here software generated MAC address is used. This carries a public key K'S chosen from a pool of onetime use keys of S'.

- *REPLY message*

A communication neighbor X receiving the POLL message will broadcast REPLY message after a time interval with a freshly generated MAC address. This also internally saves the transmission time. It contains some encrypted message with S public key (K'S). This message is called as commitment of X CX.

- *REVEAL message*

The REVEAL message broadcasting is done by using Verifier's real MAC address. It contains a map MS, a proof that S is the author of the original POLL and the verifier identity, i.e., its certified public key and signature.

- *REPORT message*

The REPORT carries X's position, the transmission time of X's REPLY, and the list of pairs of reception times and temporary identifiers referring to the REPLY broadcasts X received. The identifiers are obtained from the map MS included in the REVEAL message. Also, X discloses its own identity by including in the message its digital signature and certified public key.

1. SECURE NEIGHBOR DISCOVERY

- The Secure Neighbor Discovery (SEND) protocol is a security extension of the Neighbor Discovery Protocol (NDP) .
- Within a given distance, the nodes are identified and the communication links are recognized.
- It is susceptible to malicious interference and hence considered to be not secure. SEND provide an alternate mechanism for securing NDP with a cryptographic method that is independent of IPSec [2].
- 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.

2.POSITION VERIFICATION APPROACHES

Greedy routing and most applications in VANETs depend on reliable neighbor positions. Without position verification, nodes may declare falsified or altered positions and thereby could run several attacks, such as node segregation or packet interception.

Some approaches to verify node positions take up the basics of positioning systems. They use angle or distance measurement techniques like radio signal strength or time of flight, partly in combination with challenge-response procedures to approve position claims secure and unambiguously. The verification system contains base stations building a trustworthy network [4].

3. 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, S 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 ToF-derived mutual distances are available. In multilateration test, the unnotified links are tested. Once all couples of nodes have been checked, each node X for which two or more unnotified links exist is considered as suspect.

4. LOCATION VERIFICATION

Location verification allows nodes to have condense 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.

5. THE SECURE LOCATION VERIFICATION

The Secure Location Verification(SLV) has the capability of detecting position spoofing attacks.
SLV is an infrastructure-less cooperative scheme [3].

6. FINDING THE POSITION OF A NEIGHBOR

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 wormhole attacks.

7. CONFIRMATION OF CLAIMED POSITION

Neighbor verification schemes often rely on fixed or mobile trustworthy nodes, which are assumed to be always available for the verification of the positions announced by intruders.

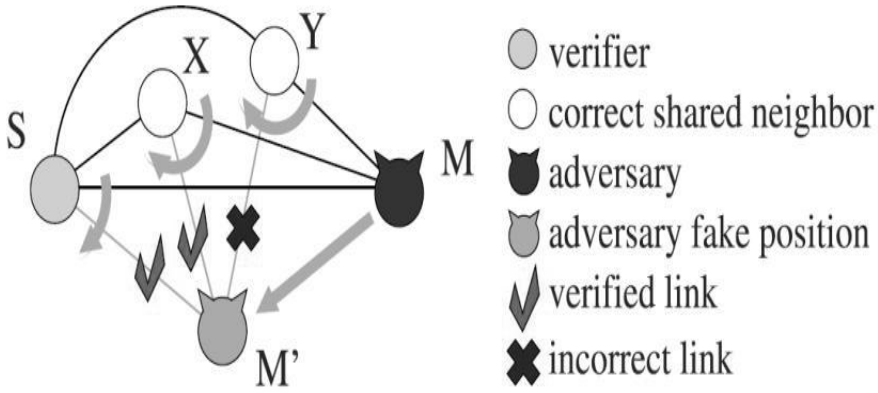

Figure 2 : Neighbor discovery in adversarial environment

8. AUTONOMOUS POSITION VERIFICATION

The location based routing protocol require that a node be able to identify its own position and position of destination node. This information is obtained via global positioning system (GPS) and location services. In the routing protocol, location information is distributed between nodes by means of position beacons.

9. IMPORTANCE OF NEIGHBOR POSITION UPDATE

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.

10. SYSTEM MODEL

The overall flow of the system is shown in the following figure, The positioning of neighbors is done and the nodes are classified. Later these positions that are claimed are verified. The new nodes are updated when they enters or leaves the range. The same verification processes are done while updating [7].

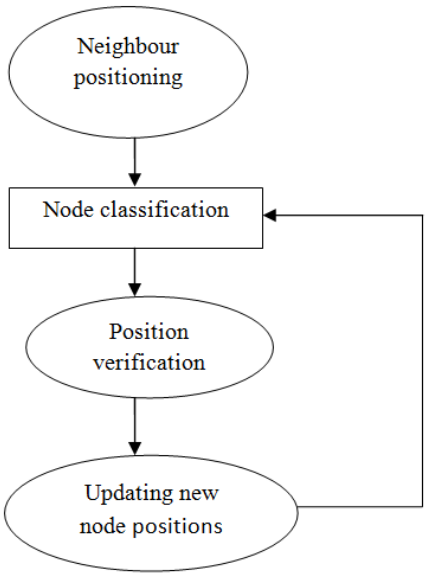

Fig 3: System flow

ADVERSARIES

Adversaries can be internal or external. Adversaries equipped with cryptographic keys and credentials that allow them to participate in the execution of the VC system protocols are termed as internal adversaries. Adversaries that do not possess keys and credentials are external adversaries. [5]

A single independent adversary cannot perform any successful attack against NPV scheme. Only Multiple independent adversaries can harm each other, thus reducing their probability of successfully announcing a false position. To rectify this problem, a new protocol is introduced namely, "Spontaneous Wireless Ad Hoc Network protocol". After identifying the position and verifying its neighbor, the next step is to exchange the information with its neighbors in a secure manner by using the spontaneous wireless ad hoc network protocol.

SECURE SPONTANEOUS PROTOCOL

A set of mobile terminals forms a spontaneous ad hoc network. It is a lightweight protocol and it is a special case 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 we consider 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 this 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. So all the nodes cannot execute the security protocols and/or routing protocols. Security methods such as pre-distribution key algorithms, symmetric and asymmetric algorithms, intermediate node- based methods and hybrid methods are not enough for spontaneous networks because, the initial configurations or external authorities are needed for the above algorithms.

Here the network and protocol can establish secure self-configured environment for resource sharing and services sharing between users. By building a trust network security has been established between users based on the service required by them. A new user can able to join the network that they belongs to. Thus the CA is distributed between users thus trust the new user. The network management is distributed to allow the network to have a distributed name services. Apply asymmetric cryptography, each device in the network has both the public and private key for device identification. Symmetric key cryptography is used to exchange the session keys between devices and nodes. Since confidentiality and validity are based on user identification, there is no anonymous users.

SECURE SPONTANEOUS NETWORK

This protocol allows the creation and management of distributed and decentralized spontaneous networks with little intervention from the user, and also different services integration. Because devices are free to join or leave the network.

In order to create the spontaneous network, the following steps should be performed:

Step 1: Joining Procedure

Step 2: Services Discovery

Step 3: Establishing Trusted Chain and changing trust level.

NETWORK CREATION

The first node in the network will be responsible for setting the global settings of the spontaneous network (SSID, session key, ...). Each node must configure its own data (including the first node): IP, port, data security, and user data. This information will allow the node to become part of the network. After this data are set in the first node, it changes to standby mode.

JOINING NEW MEMBERS

The second node first configures its user data and network security. Then, the greeting process starts. It authenticates against the first node.

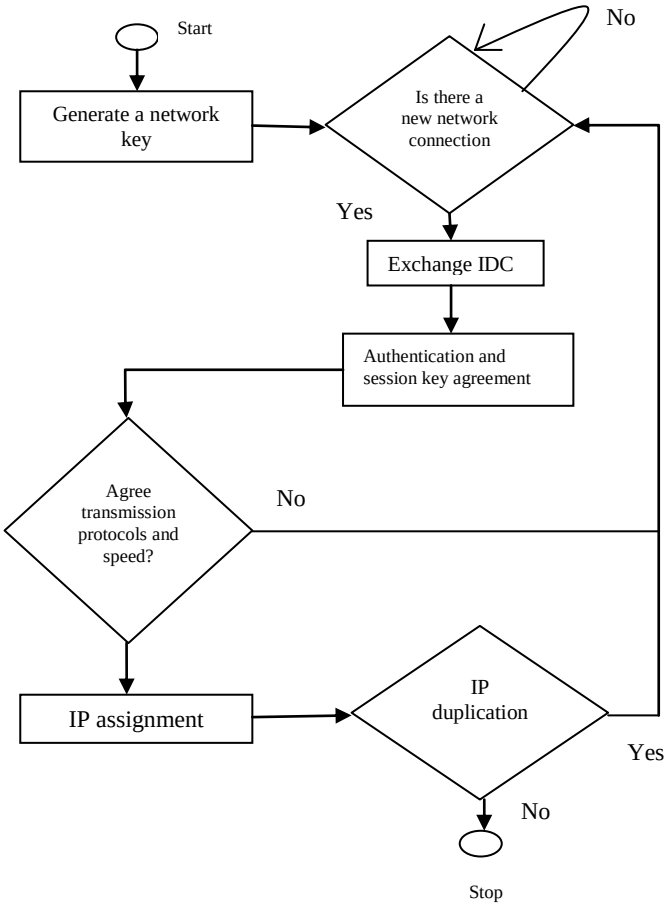

Figure 4: Algorithm for joining a new node.

II. CONCLUSIONS

The NPV 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 NPV protocol with secure spontaneous wireless Ad Hoc Network protocol,

REFERENCES

[1] Marco Fiore, Claudio Ettore Casetti, Carla-Fabiana Chiasserini, Panagiotis Papadimitratos. "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks". ieee transactions on mobile computing, vol. 12, no. 2, february 2013.

[2] http://en.wikipedia.org/wiki/Secure_Neighbor_Discovery_Protocol.

[3] J.-H. Song, V. Wong, and V. Leung, "Secure Location Verification for Vehicular Ad-Hoc Networks," Proc. IEEE Globecom, Dec. 2008.

[4] Tim T. Leinmu¨ ller, C. Maiho¨ fer, E. Schoch, and F. Kargl, "Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification," Proc. ACM Third Int'l Workshop Vehicular Ad Hoc Networks (VANET), Sept. 2006.

[5] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communications: Design and Architecture," IEEE Comm. Magazine, vol. 46, no. 11, pp. 100-109, Nov. 2008.

[6] M.Poturalski, P.Papadimitratos, and J.Hubaux, "Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility," proc.ACM Symp. Information, Computer and comm Security (ASIACCS), Mar.2008(time based verification).

[7] P.Papadimitratos, M.Poturalski, P.Lafourcade, D.Basin, S.Capkum, and J-P,Hubaux, "Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad-Hod Networks," IEEE comm.Magazine,vol.46,no.2,pp.132-39,Feb.2008.

[8] M. Mukesh and K.R. Rishi, "Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review," Int'l J. Computer Applications, vol. 12, no. 2, pp. 37-43, Dec. 2010.

[9] K. Priyadharshini , V. Kathiravan , S.Karthiga, A.Christopher Paul, "Dynamic Neighbor Positioning In Manet with Protection against Adversarial Attacks" International Journal of Computational Engineering Research||Vol, 03||Issue, 4||.

[10] S.E. Czerwinski, B.Y. Zhao, T.D. Hodes, A.D. Joseph, and R.H.Katz, "An Architecture for a Secure Service Discovery Service," Proc. ACM/IEEE MobiCom '99, Aug. 1999.

