Asian Journal of Multidisciplinary Research (AJMR) 2015

E-ISSN: 2395-1702 P-ISSN: 2395-0382
Volume 1- Issue 2-, pp-05-10

Research Paper

OPTIMIZES SECURE ROUTING AND NEIGHBOR AUTHENTICATION AND VERIFICATION IN MOBILE ADHOC NETWORK

C. Arivalai

ME Student. Department Computer Science Engineering, Chenduran Engineering College, Pudukkottai.

arivalairamesh@gmail.com

Abstract
A growing number of ad hoc networking protocols and location-aware services require that mobile nodes learn the position of their neighbors. Neighbor discovery is the process by which a node in a network determines the total number and identity of other nodesin its vicinity. In this study, issues of Mobile Adhoc Network (MANET) such as correct location establishment in the presence of attack, position verification of the neighboring nodes are handled. The challenge is to perform, in absence of trusted nodes, a fully distributed, lightweight Neighboring PositionVerification (NPV) procedure that enables each node to acquire the locations advertised by its neighbors, and assess their truthfulness. Experimental results prove that with minimal false positive rate, higher percentages of attacks are identified.

Keywords: Mobile Adhoc Network (MANET), Neighbor discovery, Neighboring Position Verification (NPV) and falsepositive rate.

1.Introduction

Generally the NPV protocols deal with the MANET where a pervasive infrastructure is not available and the node to node communication is used to find the location data's. In this case it's easy for a malicious node to enter and harm the network by using the false location information. Hence the malicious nodes are able to misuse the location based services in the wireless network. By advertising the false or forged node positions the malicious nodes could bias the geographic routing or gathering data processIn a MANET, nodes can communicate directly with each other's wireless transmission ranges. So that, a multi-hop concept produces, where various number of intermediate hosts transfer the packets which are sent by the source host before they reach the destination host. The success of communication between two nodes is highly depends on other nodes' cooperation [1].Securing protocols for mobile ad hoc networks presents unique challenges due to characteristics such as lack of pre-deployed infrastructure, centralized policy and control [2].

Location awareness is becoming an important capability for mobile computing

devices, where many protocols need knowledge of the position of the participating nodes.The correctness of node locations is therefore an important issue in mobile networks, and it becomes a challenging task in the presence of adversaries aiming at harming the system. In these cases, there is a need of solutions that let nodes

- Correctly establish their location in spite of attacks feeding false location information, and
- Verify the positions of their neighbors, so as to detect adversarial nodes announcing false locations.

In wireless networks, neighbors are usually defined as nodes that lie within radio range of each other. Thus, neighbor discovery can be considered as the exploration of the volume of space or "neighborhood" immediately surrounding a wireless node. Nodes found within the neighborhood are neighbors and, depending on network configuration and topology, may cooperate in the performance of various tasks including communications, sensing and localization. However, wireless communications are susceptible to abuse. Attackers have the freedom to perform malicious activities ranging from simple denial of service to sophisticated deception [3].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. NPV protocol is used to exchange the messages and verifies the position of communicating nodes. Some features of NPV protocols are shown below:

- It can be designed for adhoc network environment.
- It allows a node to perform all verification procedures freely.
- It is a reactive. Without prior knowledge about the neighborhood, it can be able to execute at any node, at any point and at any time.
- It is lightweight because it generates low overhead traffic.

2. Related works

Singh et al [4] discussed about the impact of bad neighbor nodes in adhoc routing and proposed a method (GNDA) for identifying good neighbornodes in the network. In addition, this approach was extended by adding extra parameters i.e. signal strength, flow capacity and relative position of a node in to the account. Proposed method optimizes the routing issues by using AODV. Result show that there was a suitable solution againstneighbor attacks.Cheneau and Laurent [5] proposed an alternate solution and introduce the Multiple-Key Cryptographically Generated Addresses (MCGA). SEND's Signature Algorithm Agility extensions were used to bind more than one Public Key to an address which enables multiple nodes to properly share and protect the same address and to resolves proxy Neighbor Discovery. Implementation results were presented and discussed the advantages of proposed approach over the existing solutions, hang and Huang [6] proposed a Jamming-Resilient Secure Neighbor Discovery schem e (JR-SND), for MANETs based on Direct Sequence Spread Spectrum and random spread code predistribution.JRSND enables neighboring nodes to securely discover each other with overwhelming probability despite the presence of omnipresent jammers. A simulation result proves the effectiveness and efficiency of JR-SND.In mobile environments, self-localization is mainly achieved through Global Navigation Satellite Systems, e.g., GPS, whose security can be provided by cryptographic and non-

cryptographic defense mechanisms [7] [8]. Alternatively, terrestrial special purpose infrastructure could be used [9], [10], along with techniques to deal with non- honest beacons [11].A mechanism for geographically assigning local broadcast keys was used to limit the range of communications. However, location-based protocols assume the availability of localization information, at least for a subset of participating nodes, making them unsuitable for scenarios without this information [3].

All existing system is not suitable for the dynamic environment as it is dependent on the position of the nodes and hence it results in the greater time delay in the ratio of data transfer. Hencethe time delay is to be eliminated and must be made to adapt to the dynamic environment.

3. System model

3.1 Neighbor Position Verification (NPV) protocol

Fig. 1 shows the message exchange with the help of NPV protocol. The shortest path is discovered using the routing protocols and that discovered shortest path is used for data transfer process. Generally the data is transmitted from source node to the destination node through several intermediate nodes. The shortest path is discovered by the 4 step message passing technique. The 4 steps are POLL, REPLY, REVEAL and REPORT messages.

- **POLL message:**A verifier S initiates this message. This message is anonymous. The verifier identity is kept hidden. Here software generated MAC addresses 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.

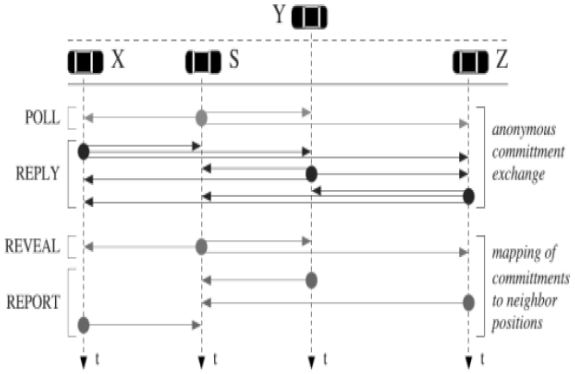

Fig. 1 Message Exchange with NVP protocol

- **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.

After performing the above mentioned four step message passing technique the shortest path is discovered. The intermediate nodes or neighbor nodes[12] in the shortest path other than the source node and destination nodes are verified whether they are real neighbor nodes or there exists any enemy nodethat is an adversary or malicious nodes in the path. At the end of the verification the nodes are reported as verifiable or enemy such as malicious or adversary or unverifiable. The process of verification helps to reduce the number of unverifiable nodes and to avoid the enemy nodes in the data transfer path. Hence it results in improving the security based on its position and the efficiency by reducing the number of unverifiable nodes.

4. Methodology

4.1 Position Verification

To verify the position of a node following three tests is to be performed which are as follows:

- Direct Symmetry Test (DST)
- Cross Symmetry Test (CST)
- The Multilateration Test (MLT)

Fig. 2 is the Neighbor discovery process in the adversary environment.

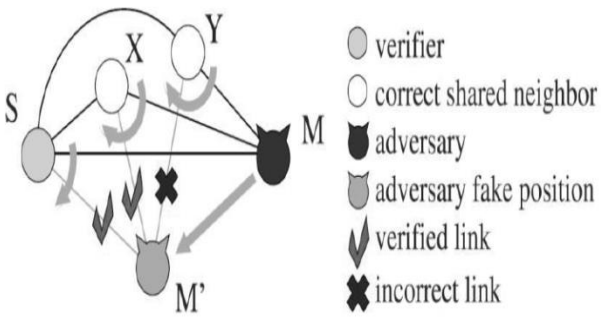

Fig. 2 Neighbor discovery in adversarial environment

In the Direct Symmetry Test, S verifies the direct links with its communication neighbors[13]. 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 is checked. This ignores nodes already declared as faulty by the DST and only considers nodes that proved to be communication neighbors between each other, that is for which ToF-derived mutual distances are available. In multilateration test, the un-notified links are tested. Once all couples of nodes have been checked, each node X for which two or more un-notified links exist is considered as suspect.

4.2 Algorithm for DST

Node S**do**

$S : F_s \leftarrow \phi$

For all $X \in N_s$ **do**

If $| d_{SX} - d_{XS} | > 2\varepsilon_r + \varepsilon_m$ **or**

$| \, ||p_S - p_X|| - d_{SX} | > 2\varepsilon_p + \varepsilon_r$

or

$d_{SX} > R$ **then**

$S : F_s \leftarrow X$

Where $||p_S - p_X||$ is the Euclidean distance between locations p_S and p_X. ε_m is the ranging error plus a tolerance value. d_{SX} and d_{XS} is the distances. Similar to tis CST, MLT is performed.

The Secure Location Verification (SLV) consists of the capability of detecting position spoofing attacks. SLV is an infrastructure-less cooperative scheme [14].

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, Secure Neighbor Discovery (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.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.

4.2 Proposed System

In the proposed work the NPV protocol is extended to meet the dynamic environment requirements. Here the mobile nodes are verified instead of verifying the position of nodes in the existing system which results in time delay and which in turn brings down the performance of the system. The mobile nodes are verified using the technique named hash function. In this if the source node, say S wants to check its neighbor for trusting it then the source node generates a hash id with the help of the function H(n)= PUB_KEY/IDENTITY and the id of the node. The neighbor node which has to be verified generates its hash id in the same way as that handled by the source node S. If the hash id of the source S and the neighbor node are same they the neighbor node is treated as trusted or verifiable else enemy node or malicious node. Here in the proposed system the Source node and the Destination nodes are also verified for the trustworthy, which is not verified in the existing system. Moreover a new technique called ERT (Elastic Routing Table) is used in the proposed work. The ERT is responsible for all the actions that are taking place in the network. This is achieved by tracing the network in the ERT instead of verifying each time.

5. Advantages

The proposed system is described and going to be implemented in such a way that it suits for all cases irrespective of its environment (Static or Dynamic). As it suits for all the environments, it significantly increases the security, performance and the rate of data transmission in the network (wired or wireless). The introduction of ERT makes the system more significant.

6. Conclusion

In this study, NPV protocol was used which allows any node in a mobile ad hoc network to verify the position of its communication neighbors without relying on a priori trustworthy nodes. 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. Proposed protocol is very robust to attacks by independent as well as colluding adversaries, even when they have perfect knowledge of the neighborhood of the verifier. Simulation results proves that proposed solution is an effective in identifying nodes advertising false positions, while keeping the probability of false positives low.

7. References

[1] R. Maheshwari, J. Gao, and S. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," Proc. IEEE INFOCOM, Apr. 2007.

[2] *Kaushik "*Analysis of MANET Security, Architecture and Assessment".

[3] Sanzgiri"Authenticated Routing for Ad hoc Networks", 2002.

[4] Stoleru "Secure Neighbor Discovery in Mobile Ad Hoc Networks",2011.

[5] Singh, U., Reddy, B. V. R., &Hoda, M. N. (2011, February). GNDA: Detecting good neighbor nodes in adhoc routing protocol. In *Emerging Applications of Information Technology (EAIT), 2011 Second International Conference on* (pp. 235-238). IEEE.

[6] Cheneau, T., & Laurent, M. (2011, May). Using SEND Signature Algorithm Agility and Multiple-Key CGA to Secure Proxy Neighbor Discovery and Anycast Addressing. In *Network and Information Systems Security (SAR-SSI), 2011 Conference on* (pp. 1-7). IEEE.

[7] Zhang, Y., & Huang, X. (2011, June). JR-SND: Jamming-resilient secure neighbor discovery in mobile ad hoc networks. In *Distributed Computing Systems (ICDCS), 2011 31st International Conference on* (pp. 529-538). IEEE.

[8] P. Papadimitratos and A. Jovanovic, "GNSS-Based Positioning: Attacks and Countermeasures," Proc. IEEE Military Comm. Conf. (MILCOM), Nov. 2008.

[9] 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.

[10] L. Lazos and R. Poovendran, "HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 233-246, Feb. 2006.

[11] R. Poovendran and L. Lazos, "A Graph Theoretic Framework for Preventing the Wormhole Attack," Wireless Networks, vol. 13, pp. 27-59, 2007.

[12] S. Zhong, M. Jadliwala, S. Upadhyaya, and C. Qiao, "Towards a Theory of Robust Localization against Malicious Beacon Nodes,"Proc. IEEE INFOCOM, Apr. 2008.

[13] Poturalski "Towards Provable Secure Neighbor Discovery in Wireless Networks", 2008.

[14] Padmavathi" A Study on Secure Spontaneous Ad Hoc Network Protocol for Neighbor Position Verification", 2013.

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