ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Collaborative Discovery and Verification of Neighbour position in MANET

R.Sagunthala[1], P.Sharmila[2], M.Somasundharam[3]

B.E. (Computer Science), SNS College of Technolore, India[1, 2, 3]

Abstract: MANET is an self configuring and infrastructure less based network. A growing number of ad hoc networking protocols and location-aware services require that mobile nodes learn the position of their neighbors. However, such a process can be easily abused or disrupted by adversarial nodes. The fully distributed cooperative NPV solution is robust against independent and colluding adversaries, and can be impaired only by an overwhelming presence of adversaries. In the existing approach, nodes are correct if they comply with the NPV protocol and adversarial if they deviate from it. Results thwart more than 99 percent of the attacks under the best possible conditions for the adversaries, with minimal false positive rates. But there is no secure message transformation. In the proposed approach secure message transformation takes place, so the trusted node informs all the correct nodes about the adversarial node, and the node will be removed from network operations cooperatively and the operational load of each correct node is reduced.

I. INTRODUCTION

A mobile ad hoc network(MANET) consists of mobile nodes or stationary nodes that communicates over wireless links and it does not have any fixed infrastructure. As dynamic topology changes are one of the characteristics of MANET. Where nodes move frequently, it rely on routing protocols. With the growing popularity of positioning devices and other localization schemes, geographic routing protocols are becoming an attractive choice for use in manet. Self-configuring infrastructureless network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. A mobile ad hoc network consists of a group of mobile nodes that communicate without requiring a fixed wireless infrastructure. It has no base station and nodes can only transmit to other nodes within link coverage. Data must be routed via intermediate nodes. A cellular network or mobile network is a wireless network distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station. compare to this network MANET has many advantages there is no need of fixed infrastructure. Mobile Ad Hoc Network (MANET) is a collection of two or more devices or nodes or terminals with wireless communications and networking capability that communicate with each other without the aid of any centralized administrator also the wireless nodes that can dynamically form a network to exchange information without using any existing fixed network infrastructure. And it's an autonomous system in which mobile hosts connected by wireless links are free to be dynamically and some time act as routers at the same time, and we discuss in this paper the distinct characteristics of traditional wired networks, including network configuration may change at any time , there is no direction or limit the movement and so on, and thus needed a new optional path Agreement (Routing Protocol) to identify nodes for these actions communicate with each other path, An ideal choice way the agreement should not only be able to find the right path, and the Ad Hoc Network must be able to adapt to changing network of this type at any time. Ad-hoc networking doesn't require any access points as opposed to wireless networks in infrastructure mode. This makes them useful in a lot of different applications. It is largely used in military applications and in rescue operations where the existing communication infrastructure has been destroyed or is unavailable, for example after earthquakes and other disasters. But ad-hoc is nowadays also being used in a lot of commercial applications, like mobile phones and PDAs using the Bluetooth protocol.

II. SECURITY

Security in wireless network is becoming more and more important while the using of mobile equipments such as cellular phones or laptops is tremendously increasing. Due to the unique characteristic of wireless network, unlike wire line networks, to achieve this goal is never a trivial challenge. Mobile ad hoc networks The cooperation between each node like a cellular phone in the network. Like all kinds of networks, passive attack and active attack are two kinds of attacks which can be launched against ad hoc networks. The passive attacks only intercept the message transmitted in the network without disturbing the transmission. The active attacks are carried out by malicious nodes which aim to disrupt transmission among other nodes or selfish nodes which may just want to save their own battery. The secure ad hoc routing protocols enhance the existing ad hoc routing protocols, such as DSR and AODV with security extensions. In these protocols, one node signs its routing messages using some cryptographic authentication method like digital signature so that each node can authenticate the legal traffic efficiently and distinguish the unauthenticated message packets from attackers and correct packets. However, there are still chances that an authenticated node has been compromised and controlled by the malicious attacker.

III. ROUTING

The main responsibilities of routing are to find the feasible path from source to destination .It is based on the criteria such as frequency path break, minimum hop length, bandwidth constraints. The correctness of node locations is therefore an all important issue in mobile networks, and it becomes particularly challenging in the presence of adversaries aiming at harming the system. Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. Determining source routes requires accumulating the address of each device between the source and destination during route discovery. The accumulated path information is cached by nodes processing the route discovery packets. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse. This may result in high overhead for long paths or large addresses, like IPv6. To avoid using source routing, DSR optionally defines a flow id option that allows packets to be forwarded on a hop-by-hop basis.

IV. RELATED WORK

Although the literature carries a multitude of ad hoc security protocols addressing a number of problems related to NPV, there are no lightweight, robust solutions to NPV that can operate autonomously in an open, ephemeral environment, without relying on trusted nodes. Securely determining own location. 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. Alternatively, terrestrial special purpose infrastructure could be used along with techniques to deal with non honest beacons [6]. We remark that this problem is orthogonal to the problem of NPV. In the rest of this paper, we will assume that devices employ one of the techniques above to securely determine their own position and time reference. Secure neighbor discovery (SND) deals with identification of nodes with which a communication link can be established or that are within a given distance .SND is only a step toward the solution we are after: simply put, 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. In other words, SND is a subset of the NPV 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. SND is most often employed to counter wormhole attacks practical solutions to the SND problem have been proposed while properties of SND protocols with proven secure solutions can be found in. Neighbor position verification was studied in the context of ad hoc and sensor networks; however, existing NPV schemes often rely on fixed or mobile trustworthy nodes, which are assumed to be always available for the verification of the positions announced by third parties. In ad hoc environments, however, the pervasive presence of either infrastructure or neighbor nodes that can be aprioristically trusted is quite unrealistic .Thus, we devise a protocol that is autonomous and does not require trustworthy neighbors. In an NPV protocol is proposed that first lets nodes calculate distances to all neighbors, and then commends that all triplets of nodes encircling a pair of other nodes act as verifiers of the pair's positions.

V. PROPOSED SYSTEM

A mobile ad hoc network, where a pervasive infrastructure is not present, and the location data must be obtained through node-to-node communication. Such a scenario is of particular interest since it leaves the door open for adversarial nodes to misuse or disrupt the location-based services. A fully-distributed, lightweight NPV procedure that enables each node to acquire the locations advertised by its neighbors, and assess their truthfulness. Secure message transformation takes place here,so the trusted node informs all the correct nodes about the adversarial node, and the node will be removed from network operations cooperatively and the operational load of each correct node is reduced.

We propose a fully distributed cooperative scheme for NPV, which enables a node, hereinafter called the verifier, to discover and verify the position of its communication neighbors. For clarity, here we summarize the principles of the protocol as well as the gist of its resilience analysis. Detailed discussions of message format, verification tests, and protocol resilience A verifier, S, can initiate the protocol at any time instant, by triggering the 4-step message exchange depicted within its 1-hop neighborhood. The aim of the message exchange is to let S collect information it can use to compute distances between any pair of its communication neighbors. To that end, POLL and REPLY messages are first broadcasted by S and its neighbors, respectively. These messages are anonymous and take advantage of the broadcast nature of the wireless medium, allowing nodes to record reciprocal timing information without disclosing their identities. Then, after a REVEAL broadcast by the verifier, nodes disclose to S, through secure and authenticated REPORT messages, their identities as well as the anonymous timing information they collected. The verifier S uses such data to match timings and identities; then, it uses the timings to perform ToF-based ranging and compute distances between all pairs of communicating nodes in its neighborhood.
Once S has derived such distances, it runs several position verification tests in order to classify each candidate neighbor as either:
1. Verified, i.e., a node the verifier deems to be at the claimed position;
2. Faulty, i.e., a node the verifier deems to have announced an incorrect position;
3. Unverifiable, i.e., a node the verifier cannot prove to be either correct or faulty, due to insufficient information.

ADVANTAGES OF PROPOSED SYSTEM:

NPV scheme is compatible with state-of the-art security architectures, including the ones that have been proposed for vehicular networks. It is lightweight, as it generates low overhead traffic. It is robust against independent and colluding adversaries. It leverages cooperation but allows a node to perform all verification procedures autonomously.

VI. CONCLUSION

We presented a distributed solution for NPV, 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. Our analysis showed that our 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 confirm that our solution is effective in identifying nodes advertising false positions, while keeping the probability of false positives low. Only an overwhelming presence of colluding adversaries in the neighborhood of the verifier, or the unlikely presence of fully collinear network topologies, can degrade the effectiveness of our NPV. The Secure message transformation takes place.

REFERENCES

[1] 1609.2-2006: IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.
[2] 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.
[3] P. Papadimitratos and A. Jovanovic, "GNSS-Based Positioning: Attacks and Countermeasures," Proc. IEEE Military Comm. Conf.(MILCOM), Nov. 2008.
[4] 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.
[5] R. Poovendran and L. Lazos, "A Graph Theoretic Framework for Preventing the Wormhole Attack," Wireless Networks, vol. 13, pp. 27-59, 2007.
[6] S. Zhong, M. Jadliwala, S. Upadhyaya, and C. Qiao, "Towards a Theory of Robust Localization against Malicious Beacon Nodes," Proc. IEEE INFOCOM, Apr. 2008.
[7] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D.Basin, S. _Capkun, and J.-P.Hubaux, "Secure Neighborhood Discovery:AFundamental Element for Mobile Ad Hoc Networks,"IEEE Comm. Magazine, vol. 46, no. 2, pp. 132-139, Feb. 2008.
[8] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defenseagainst Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, Apr. 2003.
[9] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks," Proc. IEEE 14th Int'l Conf. Network Protocols (ICNP),Nov. 2006.
[10] R. Maheshwari, J. Gao, and S. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," Proc.IEEE INFOCOM, Apr. 2007.
[11] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and J.-P. Hubaux, "A Practical Secure Neighbor Verification Protocol for Wireless Sensor Networks," Proc. Second ACM Conf. Wireless Network Security (WiSec), Mar. 2009.
[12] M. Poturalski, P. Papadimitratos, and J.-P.Hubaux, "Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), Mar. 2008.
[13] M. Poturalksi, P. Papadimitratos, and J.-P.Hubaux, "TowardsProvable Secure Neighbor Discovery in Wireless Networks," Proc.Workshop Formal Methods in Security Eng., Oct. 2008.
[14] E. Ekici, S. Vural, J. McNair, and D. Al-Abri, "Secure Probabilistic Location Verification in Randomly Deployed Wireless Sensor Networks," Elsevier Ad Hoc Networks, vol. 6, no. 2, pp. 195-209,2008.
[15] J. Chiang, J. Haas, and Y. Hu, "Secure and Precise LocationVerification Using Distance Bounding and Simultaneous Multilateration,"Proc. Second ACM Conf. Wireless Network Security (WiSec), Mar. 2009.
[16] S. _Capkun, K. Rasmussen, M. Cagalj, and M. Srivastava, "SecureLocation Verification with Hidden and Mobile Base Stations,"IEEE Trans. Mobile Computing, vol. 7, no. 4, pp. 470-483, Apr. 2008.
[17] S. _Capkun and J.-P. Hubaux, "Secure Positioning in WirelessNetworks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 221-232, Feb. 2006.
[18] A. Vora and M. Nesterenko, "Secure Location Verification UsingRadio Broadcast," IEEE Trans. Dependable and Secure Computing,vol. 3, no. 4, pp. 377-385, Oct.-Dec. 2006.
[19] J. Hwang, T. He, and Y. Kim, "Detecting Phantom Nodes inWireless Sensor Networks," Proc. IEEE INFOCOM, May 2007.
[20] 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.