Wireless Sensor Network, 2010, 2, 264-266
doi:10.4236/wsn.2010.23036 Published Online March 2010 (http://www.scirp.org/journal/wsn)

Self Umpiring System for Security in Wireless Mobile Ad Hoc Network

Ayyaswamy Kathirvel, Rengaramanujam Srinivasan
Assistant Professor, B.S.A. Crescent Engineering College, Chennai, India
Professor, B.S.A. Crescent Engineering College, Chennai, India
E-mail: {*kathir, drsrs*}*@crescentcollege.org*
Received December 22, 2009; *revised January* 6, 2010; *accepted January* 8, 2010

Abstract

A wireless mobile ad hoc network (MANET) is a self-created self-organized and self-administering set of nodes connected via wireless links without the aid of any fixed infrastructure or centralized administrator. In this paper we propose a solution of self-umpiring system that provides security for routing and data forwarding operations. In our system each node in the path from source to destination has dual roles to perform: packet forwarding and umpiring. In the umpiring role, each node in the path closely monitors the behavior of its succeeding node and if any misbehavior is noticed immediately flags off the guilty node. The umpiring system proposed is sufficiently general and can be applied to any networking protocol. For demonstration, we have implemented the self-umpiring system by modifying the popular AODV protocol. Simulation studies show that the proposed system increases throughput by 166.9% with an increase in communication overhead of 13.3% as compared to plain AODV, when 40% of the nodes are malicious and are roaming with a mobility of 20 m/s.

Keywords: MANET, Security, AODV, Self-Umpiring System

1. Introduction

A wireless mobile ad hoc network (MANET) is a self-created self-organized and self-administering set of nodes connected via wireless links without the aid of any fixed infrastructure or centralized administrator. Each node moves and operates in a distributed peer-to-peer mode, generating independent data and acting as a router to provide multi-hop communication. MANET is ideally suited for potential applications in civil and military environments, such as responses to hurricane, earthquake, tsunami, terrorism and battlefield conditions. Security is an important aspect in such mission critical applications.

In this paper we tackle the problem of securing the network layer operations from malicious nodes. Malicious nodes may disrupt routing algorithms by transmitting a false hop count; they may drop packets, route the packets through unintended routes and so on. Our work rests on the foundations of two excellent systems already proposed: the twin systems of watchdog and pathrater [1] and SCAN [2].

Our self-umpiring system has been strongly influenced by the above two schemes. In our system all the active nodes have dual roles just as in watchdog; we also exploit promiscuous hearing functionality as done by both SCAN and watchdog. We have adopted the token concept from SCAN. However we have dropped partially the pathrater functionality. We believe link reliability assessment of pathrater may not be correct; a proper reliability metric for path assessment should consider the direction and velocity of movement of active nodes. Having dropped the link reliability factor from the pathrater, the only other functionality that remains is avoidance of malicious nodes. We achieve the avoidance of malicious nodes by a system of tokens, which is similar to the ones used in SCAN. Token is a pass or validity certificate enabling a node to participate in the network. It contains two fields: nodeID and status bit; nodeID is considered to be immutable. Initially the status bit of all participating nodes is set as 0 indicating "green flag" with freedom to participate in all network operations. It is assumed that a node cannot change its own status bit. When an umpiring node finds its succeeding node misbehaving it sends a M-Error message to the source and malicious node's status bit is changed using M-Flag message (set to 1 indicating "red flag"). With "red flag" on the culprit node is prevented from participating in the network.

Copyright © 2010 SciRes.

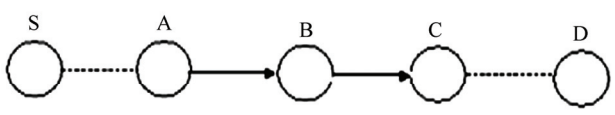
The rest of the paper is organized as follows: Section 2 provides an overview of Self_USS models. Section 3 presents simulation results; Section 4 gives the related work and Section 5 gives the conclusions

2. Self-Umpiring System Security Model: Self_Uss

In the self-umpiring system each node is issued with a token at the inception. The token consists of two fields: NodeID and status. NodeID is assumed to be unique and deemed to be beyond manipulation; status is a single bit flag. Initially the status bit is preset to zero indicating a green flag. The token with green flag is a permit issued to each node, which confers it the freedom to participate in all network activities. Each node in order to participate in any network activity, say Route Request RREQ, has to announce its token. If status bit is "1" indicating "red flag" protocol does not allow the node to participate in any network activity. The working of the self-umpiring system is explained with reference to **Figure 1**.

In the self-umpiring system all the nodes have dual roles—packet forwarding and umpiring. In the forward path during data forwarding, each node monitors the performance of immediate next node. That way, node A can tell correctly whether B is forwarding the packet sent by it, by promiscuously hearing B's transmissions. Similarly during reply process RREP, C can verify whether B is unicasting the route reply RREP and whether the hop count given by B is correct. Thus during forward path A is the umpire for B and C is the umpire for B during reverse path operations.

When a node is found to be misbehaving—say dropping packets, the corresponding umpire immediately sends a M-ERROR message to the source and the status bit of guilty node is set to "1"—red flag using M-Flag message. In order to correctly correlate the overheard messages an additional field next_hop has been introduced in all routing messages as done in SCAN [2]. Though there are several kinds of misbehavior that could be captured by promiscuous hearing we are focusing only on two types of malicious actions: dropping packets and transmitting false hop count.



During data forwarding, A is the umpire for B.
During round RREP, C is the umpire for B.

S: Source; D: Destination; A,B,C intermediate nodes

Figure 1. Self umpiring system model.

3. Simulation and Results

We use a simulation model based on QualNet 4.5 in our evaluation [3]. Our performance evaluations are based on the simulations of 100 wireless mobile nodes that form a wireless ad hoc network over a rectangular (1500 × 600 m) flat space. The MAC layer protocol used in the simulations was the Distributed Coordination Function (DCF) of IEEE 802.11 [4]. The performance setting parameters are given in **Table 1**.

Before the simulation we randomly selected a certain fraction, ranging from 0% to 40% of the network population as malicious nodes. We considered only two attacks —modifying the hop count and dropping packets. Each flow did not change its source and destination for the lifetime of a simulation run.

3.1. Throughput

In the world of MANET, packet delivery ratio has been accepted as a standard measure of throughput. Packet delivery ratio is nothing but a ratio between the numbers of packets received by the destinations to the number of packets sent by the sources.

From packet delivery ratio the following conclusions can be drawn:

1) In general packet delivery ratio decreases as mobility and percentage of malicious nodes increase.

2) We observe that the same results are obtained with Self_USS also. With zero percentage malicious nodes, self-umpiring system and plain AODV have almost identical performances.

3) We find similar increase in throughput at all other combinations of malicious node percentages and mobility values, with self-umpiring system.

From the above results we conclude that self-umpiring system leads to a substantial improvement over plain AODV, from the point of view of throughput.

3.2. Failure to Deduct (False Negatives) Probability

False Negatives Probability can be defined as:

False Negatives Probability = number of malicious nodes left undetected/total number of malicious nodes.

Table 1. Parameter settings.

Simulation Time	1500 seconds
Propagation model	Two-ray Ground Reflection
Transmission range	250 m
Bandwidth	2 Mbps
Movement model	Random way point
Maximum speed	0-20 m/s
Pause time	0 seconds
Traffic type	CBR(UDP)
Payload size	512 bytes
Number of flows	10/20

Copyright © 2010 SciRes.

The above definition requires some elaboration. We can think of two groups of malicious nodes that are left undetected. In the first group are those nodes, which never played a part in the network operation; they were probably traveling along the boundaries and never had a chance to participate in the network activity.

The second groups of malicious nodes are those that played a role as a forwarding node, but went undetected. Clearly our umpiring system is responsible only for the second group. The first group of nodes is similar to reserve players in the sidelines and clearly any umpire cannot show red flag and march off players in the sidelines. Appropriately we have done the failure to detect probability calculation taking into consideration only those nodes, which took part in the network activity. Other researchers adopt the same approach also. The results are similar that of SCAN [2].

3.3. False Accusation (False Positives) Probability

This is the probability of wrongly booking innocent nodes. We find false positive probability increases with increasing percentage of malicious nodes and increased mobility. The values vary between 0 to 10% and are similar to the patterns obtained for SCAN [2].

3.4. Communication Overhead

Communication overhead can be evaluated based on the number of transmissions of control messages like RREQ, RREP, RERR in the case of plain AODV and in addition M_ERROR, M-Flag messages in the self umpiring system. RREQ are to be decimated to the entire network, where as RREP messages are unicasts.

From communication overhead following inferences can be drawn:

1) The communication overhead increases with increasing percentage of malicious nodes and mobility for both plain AODV and Self_USS.

2) Further we find that when there is no malicious nodes (0% malicious nodes) the nodes in their umpiring role have very few message packets to send and the communication overheads for plain AODV and Self_USS are nearly same.

4. Related Works

The key distribution center (KDC) architecture is the main stream in wired network because KDC has so many merits: efficient key management, including key generation, storage, distribution and updating. The lack of trusted third party (TTPs) key management scheme is a big problem in mobile ad hoc network [5–7].

All the above schemes only try to protect the system from the attacker, but not bother about quarantining attackers. The twin systems of *watchdog* and *pathrater* [1] not only detect the mischievous nodes but also prevent their further participation in the network. SCAN [2] also has similar action, but is more comprehensive, in the sense not only packet dropping but also other misbehaviors like giving wrong hop count are covered. Our self-USS is an extension of the above two works.

Routeguard [7] is similar to *pathrater and* is run by each node. Routeguard introduces more detailed and natural classification system that rates each node into one of the five classes: *fresh, member, unstable, suspect* or *malicious.* Accordingly each node is treated differently.

5. Conclusions

A self-umpiring system for security for wireless mobile ad hoc network has been proposed. Simulation studies show that the proposed system increases throughput by 166.9% with an increase in communication overhead of 13.3% as compared to plain AODV, when 40% of the nodes are malicious and are roaming with a mobility of 20 m/s. Research work is in progress.

6. Acknowledgements

We express our thanks to Prof. V. M. Periasamy, the Register and Prof. K. M. Mehata, the Head, Department of CSE, B. S. A. Crescent Engineering College Chennai, Tamilnadu, India for the encouraging environment provided.

7. References

[1] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, Boston, USA, pp. 255–265, 6-11 August, 2000.

[2] H. Yang, J. Shu, X. Meng and S. Lu, "SCAN: Self-organized network-layer security in Mobile ad hoc networks," IEEE Journals on Selected Areas in Communications, Vol. 24, No. 2, February 2006.

[3] 3. Scalable Networks Technologies: QualNet simulator 4.5, http://www.scalable-networks.com/

[4] IEEE 802.11g. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, August, 1999.

[5] M. A. Azer, S. M. El-Kassas, and M. S. El-Soudani, "Certification and revocation schemes in ad hoc networks survey and challenges," Proceeding of IEEE International Conference on Systems and Networks Communications, 2007.

[6] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for MANET," Proceeding of International Conference on Network Protocols, pp. 251–260, 2001.

[7] N. Nasser and Y. Chen, "Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc networks," Proceeding of International Conference on Communications, pp. 1154–1159, 2007.

Copyright © 2010 SciRes.