Malicious Node Detection Mechanism for Wireless Ad Hoc Network

Daxing WANG *starleewipm@126.com*
School of Mathematical Sciences
Chuzhou University
No.1528, Feng-Le Road, Chuzhou, 239000 , Anhui, P.R. China

Abstract

With the popularity of intelligent electronics which rely on wireless communication in the post-PC era, computing devices have become cheaper, smaller, more mobile and more pervasive in daily lives. Construction of wireless ad hoc network becomes more and more convenient. However, the deployment of sensor nodes in an unattended environment makes the networks vulnerable to a variety of potential attacks. We present a malicious node detection mechanism. In using a monitoring mechanism to detect suspicious behavior, and on the basis of the responses from other monitoring nodes, if the number of suspicious entries concerning a particular node reaches a set threshold, that node is declared malicious. The simulation results show that the time it takes to detect a malicious node is decreased when there are more nodes in the network, and that it provides a fast and efficient way to detect malicious nodes.

Keywords: Ad Hoc Network, Malicious Node, Detection, Sybil Attacks, Sinkhole Attacks, Security.

1. INTRODUCTION

In the past few years, a new wireless architecture has been introduced that does not rely on any fixed infrastructure. In this architecture, all nodes may be mobile and no nodes play any special role. In fact, nodes reach other nodes they need to communicate with using their neighbors. Nodes that are close to each other discover their neighbors. When a node needs to communicate with another node, it sends the traffic to its neighbors and these neighbors pass it along towards their neighbors and so on. This repeats until the destination of the traffic is reached. Such an architecture requires that every node in the network play the role of a router by being able to determine the paths that packets needs to take in order to reach their destinations.

Wireless Ad Hoc networks are also much more dynamic and unpredictable because connectivity depends on the movements of nodes, terrain, changes in the mission (e.g. for a military application or a first responder application), node failures, weather, and other factors. As a result, it is difficult to accurately characterize normal behavior. Hence, it is often difficult to distinguish malicious behavior from normal but unexpected events. For example, a network may be seen connecting and disconnecting from the rest of the network. This may be symptomatic of an attack but can also be due to the fact that a node is moving in and out of range of the network. Existing detection tools (anomaly detection tools in particular) may not be effective in such an environment because they have been developed with a much more static and predictable environment in mind and cannot deal with the dynamism and unpredictability of MANET.

Significant research has been done in detecting intrusion in mobile ad hoc networks [1-8,10]. However, the problem of detecting a malicious node in wireless sensor networks has drawn little attention. Three known efforts towards malicious node detection are Mitigating Routing Misbehavior by Marti et al. [9], Towards Intrusion Detection in WSN by Loanis and Dimitriou [11], and Suspicious Node Detection by Signal Strength by Junior et al. [12].The method presented here addresses the mobility of sensor nodes in a hierarchical fashion in which nodes form a parent child relationship. The remainder of this paper is organized as follows. We describe proposed malicious node detection mechanism in Section II. Then we presents an evaluation of how well the proposed malicious node detection scheme performs in a multi-hop network in section III. We analyze the security of our scheme in section IV. Finally, the concluding remarks are given in Section V.

2. PROPOSED MALICIOUS NODE DETECTION MECHANISM

This In the proposed malicious node detection mechanism has been designed for the dynamic and scalable nature of sensor networks where sensor nodes are replaced once they have exhausted their energy. The message sending node observes the packet receiving node hence functioning as a monitor of the receiving node's behavior. It watches to see whether the receiving node alters the packet contents other than adding its header information. A malicious node is a compromised node where an adversary has somehow managed to break the encryption and has gained access to the secure keys and routing protocols of the Ad Hoc network. The proposed malicious node detection mechanism provides an additional countermeasure against attacks on the sensor network in the unlikely event that the secure triple key scheme is compromised. In Figure 1 a routing path has been formed from cluster leader 4 to 5 to 2 to the base station.

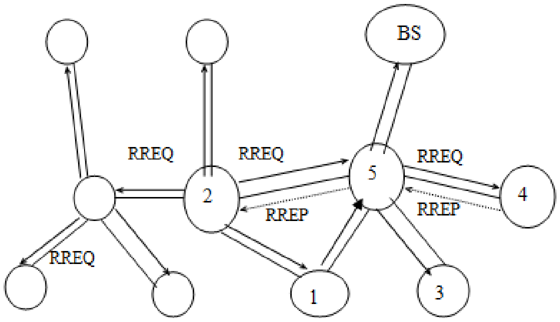

FIGURE 1: Establishment of a Routing Path.

In the proposed technique the monitoring mechanism used works as follows: Immediately after Node A sends a message to Node B, it converts itself to a monitoring node, referred to here as Am, and monitors the behavior of Node B. When Node B transmits the message to the next node, Am listens and compares this message with the one it has sent to Node B, thus establishing an original and an actual message. If the message transmitted by Node B is the same as the original then node Am ignores it and continues with its own tasks; however, if there is a difference between the original and actual messages greater than a certain threshold, the message is considered suspicious and Node B is now considered suspicious thus Node Bs.

Each node builds a Suspicious Node table containing the reputation of nodes in the cluster. Entries in this table contain the node ID, and the number of suspicious and unsuspicious entries. Nodes update this table every time they identify suspicious activity. In Table 1, ID is the unique ID of sensor node; NS denotes a suspicious node and NU is the entry for unsuspicious behavior by a node.

Node ID	Suspicious entries	Unsuspicious entries
ID	NS > 1	NU > 1

TABLE 1: Suspicious Node Table.

Each node builds its own Suspicious Node table. Every time Am identifies a suspicious entry it adds into its node suspicious table but also disseminates this information among its neighbors. Those nodes listening to the message update their Suspicious Node table. The broadcast message also acts as an inquiry to which the nodes listening reply with their statistics regarding Bs. In Figure 2 Nodes C and D are neighboring nodes of Am and Bs; they listen to the transmission from Bs and respond with a suspicious entry if the suspicious count for Bs in their Suspicious Node table is greater than its unsuspicious count; otherwise they respond with unsuspicious. Figure 3(a) shows a message sent by Node A, secured with the network key Kn while in Figure 3(b) shows an altered message from Node B.

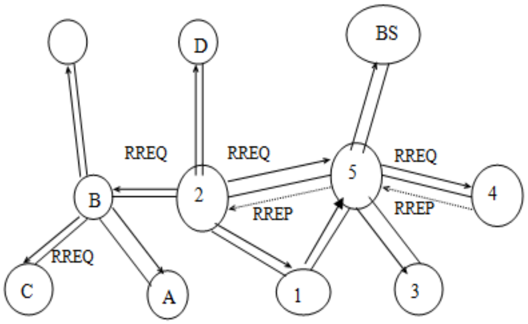

FIGURE 2: Monitoring Node Am, Suspicious Node Bs and Neighboring Nodes C&D.

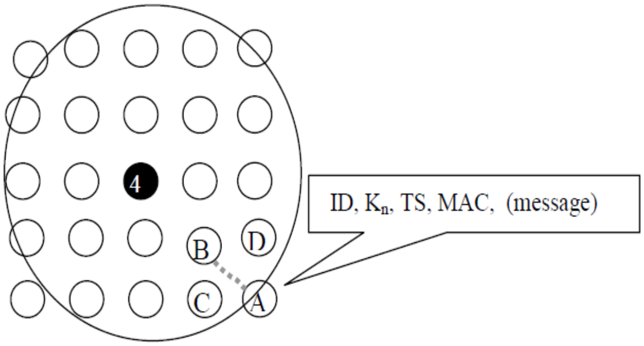

FIGURE 3: (a) Message Sent by Node A.

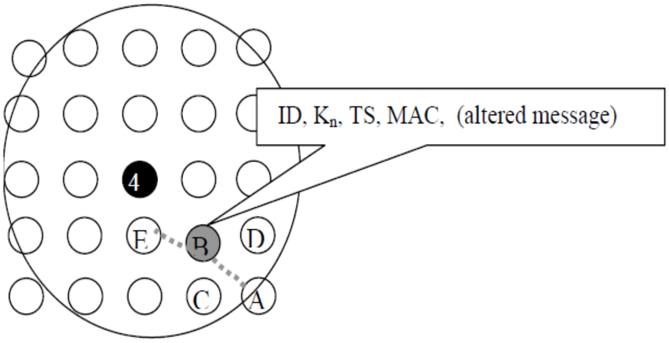

FIGURE 4: (b)Message Altered by Node B.

In each of the diagrams above, ID is the node's unique identifier, Kn is the network key, TS is an encrypted time stamp, MAC is the message authentication code generated using Kn and for message m.

Node Am collects the replies from its neighbors and updates its Suspicious Node table, it increases its own suspicious entry for Bs by one and the unsuspicious entries accordingly. Once the suspicious entries reach a certain threshold, Node Am broadcasts that Node Bs is a suspicious node and all the neighboring nodes update their Suspicious Node tables to the presence of a malicious node in the cluster. When notification of this reaches a cluster leader, it isolates Bs by erasing Bs ID from its Nodes Table and discarding any messages coming from Bs. The cluster leader also broadcasts a message saying that node Bs has been isolated, so that any message originated from Bs is immediately discarded by its neighboring nodes hence isolating and effectively removing Node Bs from the network.

3. EXPERIMENTAL EVALUATION

This section presents an evaluation of how well the proposed malicious node detection scheme performs in a multi-hop network.J-SIM was used to simulate malicious node detection. Starting with a scenario of 100 nodes randomly deployed over an area of 100×100 meters, a node transmission range of 30m was assumed. One of the nodes was to randomly become malicious. The scheme works as follows:

Neighboring nodes assess a malicious node by monitoring the actual and sent values of data. Whenever any node detects a malicious neighbor, it increases its suspicious node counter by 1 and broadcasts a message to inform other neighboring nodes. Whenever the counter reaches a threshold of 3 for a specific node, its neighbors consider that node malicious.

The sending node stays awake until the receiving node has forwarded the packet. Because of interference, this scenario might not work all the time; therefore, nodes receive a trust value from their neighbors, the threshold for which can be increased or decreased depending on the application.

Each node transfers one packet every 100 seconds. When a node receives a packet not intended for it, it first checks the destination to see whether it is for one of the neighboring nodes. If not, it discards the packet. The probability that the node stays awake to monitor its neighbors is 50%. If a malicious node is detected, the detecting node broadcasts the ID of the malicious node to its neighbors.

Once the base station has received the alert about a malicious node from at least 3 neighboring nodes, it declares the node malicious and isolates it from the network. The base station waits for the alerts from 3 nodes to ensure that the malicious node itself is not generating an alert about the legitimate nodes.

The level of this scheme’s security depends entirely on the application. The percentage of neighbors being awake all the time could be 100 percent thus providing complete security. Instead, in order to be more energy efficient, the topology works by letting each node go to sleep when it is not sending or receiving a packet.

As seen from the experimental results shown in Figure 4 below, the time required to detect a malicious node decreases when the number of nodes in the network is increased. This is because in dense network, the probability of node detection is higher and faster because there are more neighbors monitoring the nodes. The results in Figure 4 are an average of 10 runs.

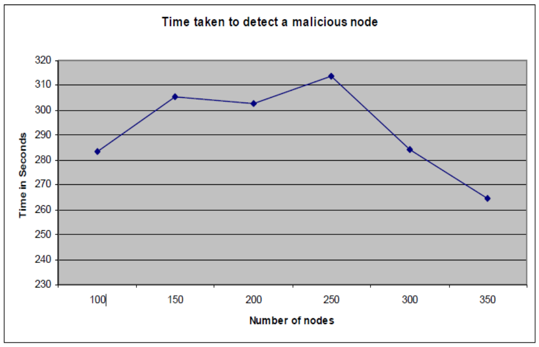

FIGURE 5: Time Taken to Detect a Malicious Node.

4. ANALYSIS OF THE PROPOSED SCHEME

The proposed malicious node detection mechanism mitigates the routing attacks discussed as follows.

4.1 Detection of Sybil Attacks

In Sybil attacks, the malicious node presents multiple identities by spoofing the identities of neighbor nodes. This attack can easily be prevented through the proposed monitoring mechanism since if Node B received a packet from Node A, Node B cannot forward this packet claiming that it is being forwarded by one of its neighbors, say Node C because the transmission is being monitored by Node A. Thus the monitoring node prevents a forwarding node from spoofing neighbor's identity.

4.2 Detection of Sinkholes, Wormholes and Selective Forwarding Attacks

In sinkhole attacks, the malicious node attracts the traffic from many nodes to pass through it by claiming to be a short route to the base station and thus acting as a sinkhole. In this attack, the malicious node is a more powerful node in terms of resources. Sinkhole attacks enable selective forwarding attacks.

4.3 Performance Metrics

In our First experiment, we vary the number of misbehaving nodes as 20,40,60,80 and 100. Our scheme achieves more delivery ratio than the [11] and [12] scheme since it has both reliability and security features. At the same time, from the results of average end-to-end delay for the misbehaving nodes 20, 40…100, our scheme has slightly lower delay than the [11] and [12] scheme because of authentication routines.

In our Second experiment, we vary the speed as 20,40,60,80 and 100, with 5 attackers. Our scheme achieves more delivery ratio than the [11] and [12] scheme since it has both reliability and security features. At the same time, from the results of average end-to-end delay for the mobility10, 20, 30, 40, and 50, we can see our scheme has slightly lower delay than the [11] and [12] scheme because of authentication routines.

The proposed monitoring mechanism detects any attempt to establish a sinkhole or wormhole by preventing the nodes from accepting any traffic from a malicious node. In addition, within the proposed framework a destination node will not accept any traffic from a source node unless it is authenticated.

5. CONCLUSION AND FUTURE WORK

The malicious node detection mechanism prevents many routing attacks such as selective forwarding, wormholes, sinkholes and Sybil attacks. In using a monitoring mechanism to detect suspicious behavior, and on the basis of the responses from other monitoring nodes, if the number of suspicious entries concerning a particular node reaches a set threshold, that node is declared malicious. This message is broadcast, alarming all the neighbors and eventually reaching the base station. The base station then isolates the malicious node and all traffic coming from that node is ignored. The simulation results show that the time it takes to detect a malicious node is decreased when there are more nodes in the network, and that it provides a fast and efficient way to detect malicious nodes.

6. ACKNOWLEDGEMENTS

This work is partially supported by the Natural Science Research Project of Education Office of Anhui Province (KJ2013B185), and the Natural Science Research Project of Chuzhou University (2012kj001Z).

We want to thank the members of our research group, who provided a lot of helpful advice for this paper.

7. REFERENCES

[1] Patrick S. Chen, Shing-Han Li and Yung-Kuei Liu, “Scheduling the Access to Multi-Level Secure Databases in a Wireless Network Environment”, International Journal of Innovative Computing, Information and Control (IJICIC), vol.6, no. 12,pp.5381-5404, 2011.

[2] Samuel Madden, Michael J. Franklin, Joseph M. Hellerstein, “An Acquisitional Query Processing System for Sensor Networks”. ACM Trans. Database Syst., 30(1):122–173, 2005.

[3] M. Palomera-Perez, H. Benitez-Perez and J. Ortega-Arjona, “Coordinated Tasks: A Framework for Distributed Tasks in Mobile Area Networks”, ICIC Express Letters, Volume 5, Issue 8(B), pp.3941-3946, 2011.pp.2817-2824,2011.

[4] Xueyan Tang and Jianliang Xu. “Optimizing lifetime for continuous data aggregation with precision guarantees in wireless sensor networks”. IEEE/ACM Trans. 16(4):904–917, 2008.

[5] Yingqi Xu, Tao-Yang Fu, Wang-Chien Lee, “Processing k nearest neighbor queries in location-aware sensor networks”. Signal Processing, 87(12):2861–2881, 2007.

[6] Jilong XUE, Xiaogang QI, Chenyu WANG. “An Energy-Balance Routing Algorithm Based on Node Classification for Wireless Sensor Networks”. Journal of Computational Information Systems, Vol. 7 (7): 2277- 2284, 2011.

[7] Yiliang Han, Xiaolin Gui and Xuguang Wu, “Parallel Multi-Recipient Signcryption for Imbalanced Wireless Networks”, International Journal of Innovative Computing, Information and Control (IJICIC), vol.6, no.8,pp.3521-3630, 2010.

[8] Mustafa Fayomi, “An enhancement of authentication protocol and key agreement (AKA) for 3G mobile networks”. International Journal of Security, Vol. 5 (1): 35- 61, 2011.

[9] Marti, S., T. J., Lai, K. and Baker, M. “Mitigating routing misbehavior in mobile ad hoc networks”. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom 2000) August 6-11, 2000, Boston, USA. Boston, MA, ACM Press, pp. 255-265.

[10] Aamir Shahzad, “Cryptography and authentication placement to provide secure channel for SCADA communication”, International Journal of Security, Vol. 6 (3): 28- 44, 2012.

[11] Loanis, K. and Dimitrou, T. “Towards intrusion detection in wireless sensor networks”. In Proceedings of the 13th European Wireless Conference, April 1-4, 2007, Paris, France.

[12] Junior, W., Figueiredo, T. and Wong, H. “Malicious node detection in wireless sensor networks”. In Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS’04), April 26-30, 2004, Santa Fe, New Mexico.