International Journal of Advance Research, IJOAR .org
Volume 1, Issue 7, July 2013, Online: ISSN 2320-9119

WIRELESS AD HOC NETWORKS: MALICIOUS NODE DETECTION

Dr. R. Hashemnejad, Dr.K.Purushothaman

ABSTRACT

With the recognition of intelligent physics that think about wireless communication within the post-PC era, computing devices became cheaper, smaller, a lot of mobile and a lot of pervasive in daily lives. Construction of the wireless circumstantial network becomes a lot more convenient. However, the readying of device nodes in unattended setting makes the networks liable for a range of potential attacks. We tend to gift a malicious node detection mechanism. In employing an observance mechanism to observe suspicious behavior, and on the idea of the responses from different observance nodes, if the quantity of suspicious entries regarding a selected node reaches a collection threshold, that node is asserted malicious. The simulation results show that the time it takes to observe a malicious node is attenuated once there are a lot of nodes within the network, which it provides a quick and economical means to observe malicious nodes.

Keywords:

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

INTRODUCTION

In the past few years, a brand new wireless design has been introduced that doesn't place confidence in any security infrastructure. In designing of this, all nodes could also be mobile and no nodes play any special role. In fact, nodes reach different nodes they have to empathize with utilization of their neighbors. Nodes that are near one another discover their neighbors. Once a node has to communicate with another node, it sends the traffic to its neighbors and these neighbors pass it on towards their neighbors and then on. This repeats till the destination of the traffic is reached. Such a design requires that each node within the network play the role of a router by having the ability to work out the ways that packets have to soak up in order to achieve their destinations.

Wireless Ad Hoc networks also are rather more dynamic and unpredictable as a result of property, which depends on the movements of nodes, terrain, changes within the mission (e.g. For a military application or a primary communicator application), node failures, weather, and different factors. As a result, it is troublesome to accurately characterize the traditional behavior. Hence, it's typically troublesome to differentiate malicious behavior from traditional however surprising events. For instance, a network could also be seen connecting and disconnecting from the remainder of the network. This might be characteristic. An attack however also can result to the very fact that a node is acquiring and out of vary of the network. Existing detection tools (anomaly detection tools in particular) might not be effective in such kind of atmosphere as a result of their need been developed with away a lot of static and predictable atmosphere in mind and cannot manage the dynamism and unpredictability of the MANET.

Significant analysis has been worn out sleuthing intrusion in mobile Ad Hoc networks. However, the matter of sleuthing a malicious node in wireless detector networks has drawn very little attention. Renowned efforts towards malicious node detection are mitigating routing misdeed by Marti et al. Towards Intrusion Detection in WSN by Loanis and Dimitriou, and Suspicious Node Detection by Signal Strength by Junior et al. The method bestowed here addresses the quality of detector nodes in an exceedingly class-conscious

fashion during which nodes are in a kind of parent kid relationship. The rest of this paper is organized as follows. We have a tendency to describe planned malicious node detection mechanism. Presents an analysis of however well the planned malicious node detection theme performs in an exceedingly multi-hop network in section, we have a to analyze the safety. Finally, the last remarks are described at the end.

MALICIOUS NODE DETECTION MECHANISM

Within the proposed malicious node detection mechanism is designed for the dynamic and climbable nature of detector networks where detector nodes are replaced once they have exhausted their energy. The message causing 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 aside from adding its header information. A malicious node may be a compromised node where resister has somehow managed to interrupt the coding and has gained access to the secure keys and routing protocols of the unintended network. The proposed malicious node detection mechanism provides a further measure against attacks on the detector network within the unlikely event that the secure triple key theme is compromised. In Figure one a routing path has been shaped from cluster leader 4 to five to 2 to the base station.

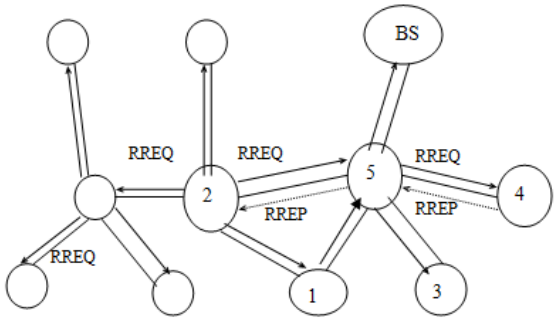

FIGURE 1: Establishment of a Routing Path.

In the planned technique the observed mechanism used works as follows: straightaway when Node A sends a message to Node B, it converts itself to an observance node, brought up here as Am, and monitors the behavior of Node B. Once Node B transmits the message

to consecutive node, Am listens and compares this message with the one it has sent to Node B, so establishing an imaginative associated an actual message. If the message transmitted by Node B is that the same because the original then node Am ignores it and continues with its own tasks; but, if there's a distinction between the initial and actual messages bigger than a particular threshold, the message thought is taken into account as suspicious and Node B is currently considered suspicious so 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 therefore the range of suspicious and trusting entries. Nodes update this table each time they establish suspicious activity. In Table 1, ID is the unique ID of sensor node; NS denotes a suspicious node and alphabetic character is the entry for trusting 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 updates their Suspicious Node table. The broadcast message additionally acts as an inquiry to that the nodes listening reply with their statistics concerning. In Figure a pair of Nodes C and D are neighboring nodes of Am and BS and they hear the transmission from the BS and respond to a suspicious entry if the suspicious count for bias in their Suspicious Node table is bigger than its unsuspecting count, otherwise they respond with unsuspecting. Figure 3 (a) shows a message sent by Node A, secured with the network key knee while in Figure 3

(b) shows AN altered message from Node B.

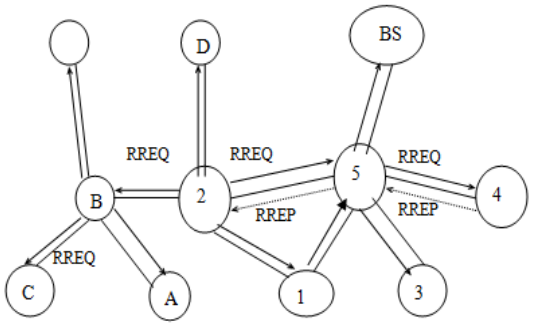

FIGURE 2: Monitoring Node Am, Suspicious Node Bs and Neighboring Nodes C&D.

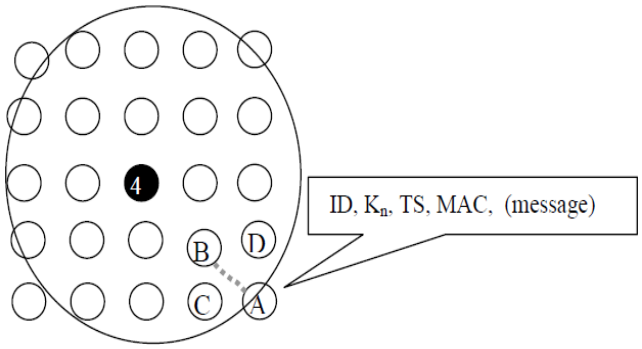

FIGURE 3: (a) Message Sent by Node A.

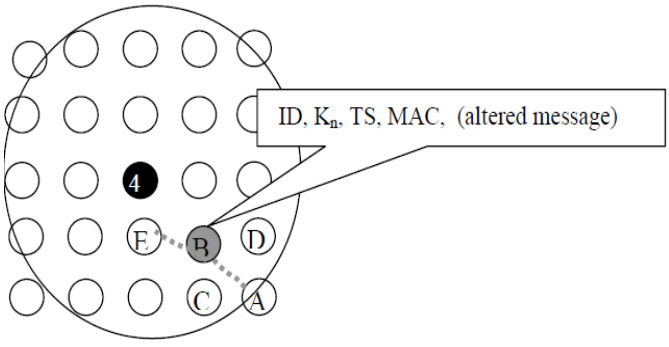

FIGURE 4: (b)Message Altered by Node B.

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 also the unsuspicious entries accordingly. Once the suspicious entries reach a precise threshold, Node Am broadcasts that Node Bs may be a suspicious node and all the neighboring nodes update their suspicious Node tables to the presence of a malicious node within 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 conjointly broadcasts a message locution that node BS has been isolated, in order that any message originated from BS is straight away discarded by its neighboring nodes hence analytic and effectively removing Node BS from the network.

EXPERIMENTAL EVALUATION

This section presents an analysis of how well the proposed malicious node detection scheme performs in an exceedingly multi-hop network. J-SIM was employed to simulate the malicious node detection. Beginning with a situation of 100 nodes haphazardly deployed over a section of 100×100 meters, a node transmission range of 30m was assumed. One in all the nodes was to haphazardly become malicious. The scheme works as follows:

Neighboring nodes assess a malicious node by observation of the genuine and transmitted values of data. Whenever any node detects a malicious neighbor, it enhances its suspicious node counter by 1 and broadcasts a message to tell other neighboring nodes. Whenever the counter reaches a threshold of 3 for a particular node, its neighbors think about that node malicious.

The causing node stays awake until the receiving node has forwarded the packet. Due to interference, this situation may not work all the time; thus, nodes receive a trust's price from their neighbors, the brink of which will be redoubled or shrunken relying on the applying.

Each node transfers one packet every 100 seconds. Once a node receives a packet not supposed to it, it primarily checks the destination to visualize whether it is for one in all the neighboring nodes. If not, it discards the packet. The likelihood that the node stays responsive to monitor its neighbors are five hundredth. If a malicious node is detected, the detecting node transmits the ID of the malicious node to its neighbors.

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

The level of this scheme's security relies entirely on the applying. The share of neighbors being awake all the time could be one hundred percent thus providing complete security. Instead, so as to be additionally energy economy, the topology works by allowing each node to rest when it is not transferred or getting pecked.

As seen from the experimental results shown in Figure 4 below, the time required to notice a malicious node decreases once the traffic of nodes in the network is redoubled. This is as a result of in dense network, the likelihood of node detection is higher and faster as a result there is additional neighbors observing modes. The results in Figure 4 are a mean of ten runs.

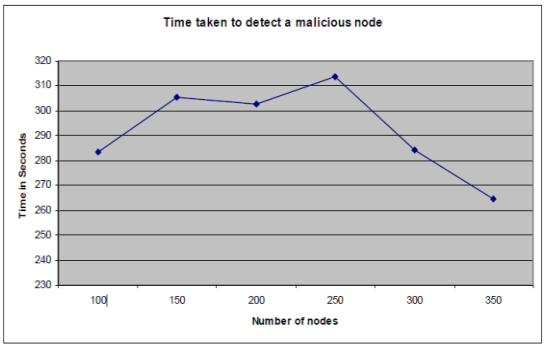

FIGURE 5: Time Taken to identify a Malicious Node.

ANALYSIS OF THE PROPOSED SCHEME

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

1 Detection of Sybil Attacks

In Sybil attacks, the malicious node presents multiple identities by spoofing the identities of neighbor nodes. This attack will simply be prevented through the projected 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 in all its neighbors, say Node C as a result of the transmission is being monitored by Node A. Therefore the monitoring node prevents a forwarding node from spoofing neighbor's identity.

2 Detection of Sinkholes, Wormholes and Selective Forwarding Attacks

In depression attacks, the malicious node attracts the traffic from several nodes to suffer it by claiming to be a short route to the base station and therefore acting as a depression. During this attack, the malicious node could be an additional powerful node in terms of resources. Depression attacks alter selective forwarding attacks.

3 Performance Metrics

In our initial experiment, we tend to vary the quantity of misbehaving nodes as 20,40,60,80 and 100. Our team achieves an additional delivery ratio than the [11] and

[12] theme since it has both dependability and safety features. At the same time, from the results of average end-to-end delay for the misbehaving nodes 20, 40…100, our theme has a slightly lower delay than the [11] and [12] theme attributable to authentication routines.

In our Second experiment, we tend to vary the speed as 20,40,60,80 and 100, with five attackers. Our team achieves an additional delivery ratio than the [11] and [12] theme since it has both dependability and safety features. At the same time, from the results of average end-to-end delay for the mobility10, 20, 30, 40, and 50, we are able to see our theme has a slightly lower delay than the [11] and [12] theme attributable to authentication routines.

The projected monitoring mechanism detects any efforts to establish a depression or hole by preventing the nodes from accepting any traffic from a malicious node. Additionally, within the projected framework, a destination node won't accept any traffic from a supply node unless it is documented.

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 watching mechanism to observe suspicious behavior, and on the idea of the responses from alternative watching nodes, if the number of suspicious entries concerning a specific node reaches a collection threshold, that node is declared malicious. This message is broadcast as ominous to all the neighbors and eventually reaching the bottom station. The bottom station then isolates the malicious node and all traffic coming back from that node is neglected. The simulation results show that the time it takes to observe a malicious node is diminished once there are additional nodes within the network, which it provides a quick and efficient way to observe malicious nodes.

REFERENCES

[1] Rajasekaran, K., & Balasubramanian, K. Performance Evaluation on Secure Transaction Protocols in WSN. International Journal of Scientific & Engineering Research

[2] David, J., & Jayasingh, R. Novel Defense Scheme for Static and Dynamic Wireless Mess Network. International Journal of Scientific & Engineering Research

[3] Singh, M., & Das, R. A Survey of Different Techniques for Detection of Wormhole Attack in Wireless Sensor Network. International Journal of Scientific & Engineering Research

[4] ROOPAK, M., & Reddy, B. V. R. BLACKHOLE ATTACK IMPLEMENTATION IN AODV ROUTING PROTOCOL. International Journal of Scientific & Engineering Research

[5] Ashoor, A. S., & Gore, S. Intrusion Detection System (IDS) &Intrusion Prevention System (IPS): Case Study. International Journal of Scientific & Engineering Research, 2.

[6] Santhosh Krishna, B. V., & AL, M. V. Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism. International Journal of Scientific & Engineering Research

[7] Abel, V. (2011). Survey of Current and Future Trends in Security in Wireless Networks. International Journal of Scientific & Engineering Research (ISSN 2229-5518)

[8] WANG, D. (2013). Malicious Node Detection Mechanism for Wireless Ad Hoc Network. International Journal of Security (IJS), 7 (1),

[9] Zhang, Y., & Lee, W. (2000, August). Intrusion detection in wireless ad-hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 275-283). ACM.

[10] Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. Communications Magazine, IEEE, 40 (10), 70-75.

[11] Papadimitratos, P., & Haas, Z. J. (2002). Secure routing for mobile ad hoc networks. In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS) (pp. 193-204).

[12] Marti, S., Giuli, T. J., la, K., & Baker, M. (2000, August). Mitigating routing misbehavior in mobile ad hoc networks. In International Conference on Mobile Computing and Networking: Proceedings of the 6 th annual international conference on Mobile computing and networking (Vol. 6, No. 11, pp. 255-265).

[13] Mishra, A., Nadkarni, K., & Patcha, A. (2004). Intrusion detection in wireless ad hoc networks. Wireless Communications, IEEE, 11 (1), 48-60.