

Malicious Attacks detection in Wireless Ad Hoc Networks By using SNDP protocol

Abhishek Ranjan
Department of IT
Botho College
Gabrone, Botswana

Email- abhishek.ranjan@bothocollege.ac.bw

Rajalakshmi Selvaraj
Department of IT
Botho College
Gabrone, Botswana

Email- rajalakshmi.selvaraj@bothocollege.ac.bw

ABSTRACT:

In this research to detect the Stealthy Attacks such as misrouting, power control, identity delegation, and colluding collision. Those kinds of attacks easily launched against Multihop wireless ad hoc networks. When every the source and destination are communicate, to appear Stealthy Attacks and dropping or interrupt the packet from reaching the destination through malicious behavior node. To overcome this problem we can present a protocol called SNDP (secure neighbor discovery protocol) that can detect and isolate stealthy packet dropping attack efficiently.

Keywords: Misrouting, Power Control, Identity Delegation, and Colluding Collision, Guard node and SNDP protocol.

I. INTRODUCTION

In generally the WIRELESS Ad hoc and Sensor Networks (WASN) is most important platform in more than a few domains such as military warfare and control of civilian critical infrastructure. In these networks the malicious behavior node gives the impression to its neighbors that it

performs the legitimate forwarding action.

We provide the secure neighbor discovery protocol (SNDP) that is built against stealthy attack. This kind of protocol easily detects the attackers and controls the stealthy attacker's behaviors. The SNDP detection technique having two different principles; first, when ever the source and destination nodes are communicated the guard node to establish the route path and distribute the key form transmission path. Second the each and every node having some checking responsibility to each neighbor. Based on this technique to detect the four attacks and neighbors have differing views of a node in terms of the amount of forwarding traffic generated by that node. Hence, a multi-hop broadcast cannot convince all the neighbors, than we will show that of the four modes of the stealthy packet dropping attack and behaviours. To our contributions in this paper as follows;

1. We will describes the stealthy attack and misbehavior like packet dropping class of attacks and detail four attack methods by which it can be arrived on wireless sensor networks.

2. We provide the SNDP protocol against stealthy attacks with added the resource consumption and node responsibility.

3. We show through analysis and simulations the security advantage of SNDP protocol in wireless sensor networks.

The research design of this paper as follows: section 3. We will describe the stealthy attacks model such as four attacks. Section 4 we will discuss the stealthy attack detection by using SNDP protocol. Section 5 we will shows the experimental evaluations for SNDP protocol. Finally describes the conclusion of this research.

III. Stealthy Attacks model:

In this section III will describes the four types of stealthy attacks such as misrouting, power control, identity delegation, and colluding collision are follows:

A. Misrouting:

We will study four principal types of attacks. In a *first* type of attack, the Misrouting wishes to chance the path dimension. This type of attack can't be misrouting the full data but only misrouting the packet between sources to destination. In this mode, Misrouting attack relays the packet to an incorrect next-hop neighbor and also destination node doesn't receive the full data packets.

B. Power control:

In a *second* type of stealth attack, the Power control attack in order to reduce the Power level form legitimate nodes. In this mode, malicious node controls the transmission power to relay the packet form the intermediate node. In this process the packet does not reach the next hop while the attacker occurred.

C. colluding collision:

In a *Third* type of stealth attack, the colluding collision attack. When ever the source node transmit data packets to destination node, the same time malicious node to transmit the same or different request form source node. Therefore, a collision occurs at Source node.

D. Identity delegation:

The final type of stealth attack is called identity delegation attack. In this mode, the attacker can act as any intermediate node or destination. Here the legitimate node doesn't receive data packets because the malicious behaviours nodes can access the particular data packets.

<i>Attack Name</i>	<i>Attack process</i>	<i>Attack requirement and its problem</i>
Misrouting	Change path dimension	It requires any intermediate node and Destination doesn't receive data
Power control	Continuously send the data (hello packet)	Intermediate node loss the energy and packet will loss
Colluding	Continuously	Collision

collision	request to source	acquire in source node
identity delegation	Identify legitimate nodes	Act as any intermediate or destination node

Table 1 stealthy attack model description

IV. SNDP Protocol Model

When ever the attackers can utilize malicious behaviours node that time the guard as doing its forwarding job correctly. In this **secure neighbor discovery protocol (SNDP)** provides the authorized path between source and destination node by help of guard node and also distributed the key only for authorized node because the guard node monitor the overall wireless networks. In this wireless network the each and every neighbor has some checking responsibility through out “hello packets” and neighbor discovery & neighbor verification perform the overall network by using key values.

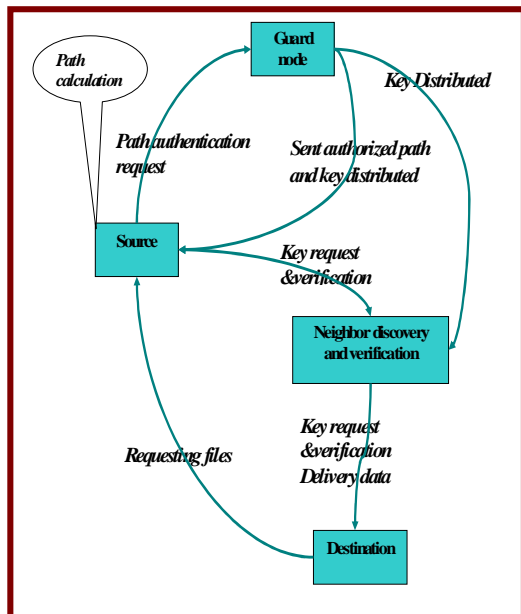


Figure 1 SNDP Framework

The SNDP secure neighbor discovery protocol Framework having some set of procedures is follows and supported to reduce the malicious node behaviours and its problems.

Step 1: The first to construct the wireless sensor network and its more information are given following section in figure 2.

Step 2: After constructing wireless sensor network to elect the guard node. Here guard’s nodes do the correct job (forwarding data packets through out neighbor’s nodes)

Step 3: To select any node and act as source node and destination node from the wireless sensor network.

Step 4: When ever the destination node request to the source node. It finds out the shortest path between the source and destination node by using shortest path algorithm.

Step 5: After completing the shortest path finding process the source will request to guard node and its message as “path Authentication request”.

Step 6: when every the guard node to receiving the path Authentication request, it will generate the authorized path based on shortest path information.

Step 7: The guard node will distribute the key into source node, destination node and its neighbor who are placed into authorized path information.

Step 8: Before sending data the source node should be request to its neighbor node.

Step 9: The intermediates node collect the “key request” information. In case the intermediate node having key means

it will reply the “key” form the source node.

Step 10: The source node to collect the particular key and check the key values based on guard node distributed key values. The key values are matched means it send the data packets otherwise the source node does not transmitted the data packets form its neighbor nodes.

Step 11: After collecting the data packets the neighbor node again request to its node neighbor’s and transmitted the “key request” and another node to receive the message and reply the key up to destination the same process will be executed and authenticates the overall wireless sensor network.

Step 12: Finally the destination node receive the data packets with the help of guard node. The same manner another kind pf source node and destination node are communicate and transmitted data packets.

V. Experimental Evaluations

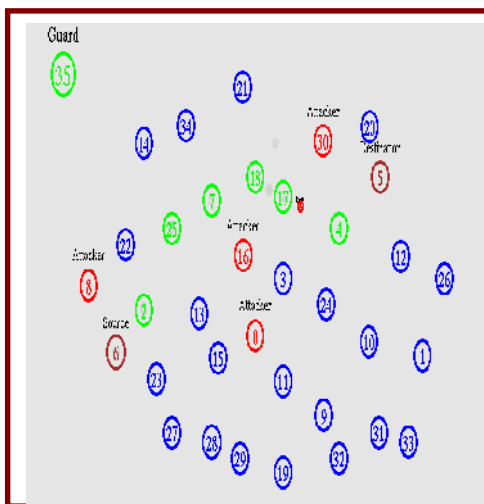


Figure 2 wireless network frameworks

For example, the above wireless network to construct by 35 nodes, here one node act as the guard node and its monitor the

overall networks. The Following steps to describe the work process details:

Step 1: The destination node request to source node.

Step 2: The source node send the authorized path form guard node.

Step 3: The guard node already identify the information about the both legitimate nodes and malicious nodes behaviours.

Step 4: The guard node to find out the authorized path and also distributed the key form authorized path.

Step 5: Before transmit the data packets, the source node send the “hello packets” to its neighbor node.

Step 6: The neighbor node reply into two ways:

- Hello packets with key
- Hello packets without key

Step 7: The node having key means it going to set the “active” state Otherwise reaming node are moves to “sleep” state.

Step 8: up to destination same process will be executed.

Step 9: finally the data packets delivered without loss.

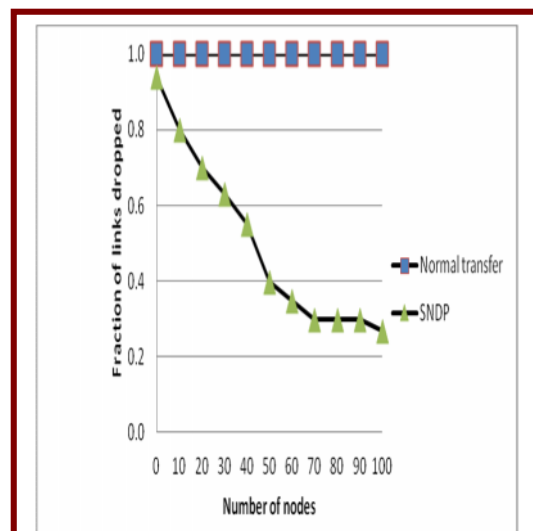


Figure 3 Delivery ratios Comparison with Normal node

The figure 3 to describe the fraction of link dropped comparison between the normal transfer and SNDP protocols. In normal transaction process are use the some other protocol, but the dropped links are high to compare the SNDP protocol. Here the total number of node 100 will communicates with each other but the high links are dropped in normal protocol. The secure neighbor discovery protocol (SNDP) to reduce the dropped link compare to some other protocol.

The normal transfer wireless sensor network unnecessary to loss the data packets because the redundant dropped links are appeared. To overcome this problem to use the SNDP protocol reduces the unnecessary packet loss. The comparison graph show on figure 3.

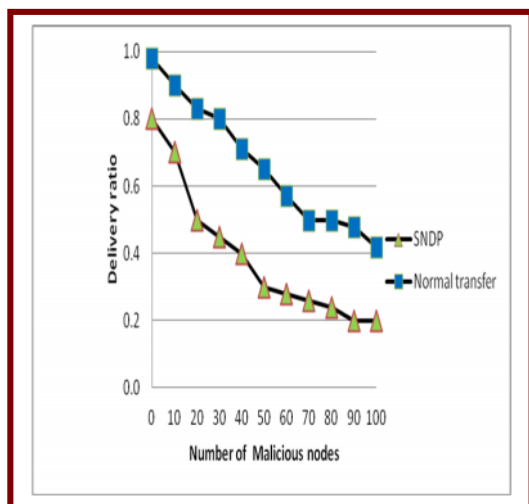


Figure 4 Delivery ratios Comparison with Malicious node & Normal node

In Figure 4 will represent the Comparison delivery ratios between the malicious node & Normal node. In case the wireless sensor network uses some other protocol that time the malicious node increase the delivery ratio form their network. To overcomes this problem to reducing the unnecessary loss to data packets from their network by using SNDP protocol and its framework. The SNDP framework to support to reduces the malicious node delivery ratio form their network to compare any another protocol or normal transfer the simulation comparison graph show on figure 4.

Conclusion

We can describes the four kind of attacks called stealthy packet such as misrouting, power control, identity delegation, and colluding collision which all are making dropping the data packets and also disrupts a packet from reaching the destination by malicious behavior at an intermediate node. However, the malicious behavior cannot be detected easily by any kind of protocols. In this detection approach and its framework to expand into neighbors that are capable of monitoring in a neighborhood, thereby making it more suitable than other protocols. We showed through analysis and simulation that SNDP protocol and its behaviours than we showed that comparison between the some any other protocol and SNDP protocol. In future we can plan to analyze the impact of the detection technique on the network

throughput under different adversary models.

References

- [1] DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks, David B. Johnson David A. Maltz Josh Broch
- [2] I. Khalil and S. Bagchi, "MISPAR: Mitigating Stealthy Packet Dropping in Locally-Monitored Multi-Hop Wireless Ad Hoc Networks," Proc. ACM Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), <http://doi.acm.org/10.1145/1460877.1460913>, 2008.
- [3] Secure Neighbor Discovery in Wireless Sensor Networks Saurabh Bagchi Purdue University, sbagchi@purdue.edu Srikanth Hariharan Purdue University, srikanth@purdue.edu Ness Shroff Purdue University, shroff@purdue.edu
- [4] C. Hartung, R. Han, C. Seielstad, and S. Holbrook, "FireWxNet: A Multi-Tiered Portable Wireless System for Monitoring Weather Conditions in Wildland Fire Environments," Proc. ACM MobiSys, pp. 28-41, 2006.
- [5] S. Ganeriwal, L.K. Balzano, and M.B. Srivastava, "Reputation- Based Framework for High Integrity Sensor Networks," ACM Trans. Sensor Networks, vol. 4, no. 3, pp. 1-37, <http://doi.acm.org/10.1145/1362542.1362546>, May 2008.
- [6] D. Johnson, D. Maltz, and J. Broch, "The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," Ad Hoc Networking, Addison-Wesley, 2001.
- [7] C.E. Perkins and E.M. Royer, "Ad-Hoc on Demand Distance Vector Routing," Proc. Second IEEE Workshop Mobile Computing Systems and Applications (WMCSA '99), pp. 90-100, 1999.
- [8] D. Ganesan, B. Krishnamurthy, A. Woo, D. Culler, D. Estrin, and S. Wicker, "An Empirical Study of Epidemic Algorithms in Large Scale Multihop Wireless Networks," Technical Report Intel IRPTR- 02-003, Intel Research, Mar. 2002.
- [9] F. Ye, H. Luo, J. Cheng, S. Lu, and L. Zhang, "A Two-Tier Data Dissemination Model for Large-Scale Wireless Sensor Network," Proc. Eighth ACM Ann. Conf. Mobile Computing and Networking, pp. 148-159, 2002
- [10] Q. Zhang, P. Wang, D. Reeves, and P. Ning, "Defending against Sybil Attacks in Sensor Networks," Proc. Int'l Workshop Security in Distributed Computing Systems (SDCS '05), pp. 185-191, and 2005.

