RPB (Reverse Path Based) Approach to Detect and Prevent Black Hole Attacks in WSN

Avneet Kaur
M.Tech, CSE, CGC Landran, India.

Mandeep Kaur
Asstt. Professor, CEC, Landran, India.

Harneet Kaur
Asstt. Professor, CEC, Landran, India.

Abstract – This paper is based on black-hole detection and prevention in the Wireless Sensor Nodes (WSN's). This is an attack occurs cause of malicious nodes, which fetch the data packets by falsely advertising a false route to the destination. Wireless networks are very popular these days, as the users want wireless connectivity at every geographic position. There is an increasing problem of attacks on Wireless Sensor Nodes (WSN's) Black hole attack is one of the security loophole in which the traffic is redirected to unauthorized node that actually does not exist in the network. The nodes represent itself in the way to the other nodes that it can attack other nodes and networks knowing that it has the shortest path. WSN must have a secure way for communication, which is pretty challenging. By aiming to provide secure communication and transmission, researchers working specifically on the security threats in WSN, and provide us secure routing protocols.

Index Terms – MANET, Black Hole, and Routing Protocols.

1. INTRODUCTION

A wireless sensor network (WSN) is a group of sensor nodes spread over a specific area where the changes would be observed. A wireless sensor network contains of sensing elements; storage component, processing unit and these nodes can interact with the other nodes too. All sensor nodes communicate through a wireless transmission. The sensor nodes are randomly plotted in the area. If the sensor node is not able to communicate to the other node through an explicit link, i.e. it means they are out of broadcasting range; the packet can be sent to that node by using the intermediate nodes. The concept of using the intermediary nodes to transmit the data is called as multi-hopping. There is no requirement to provide an infrastructure to set up the network, as the wireless sensor networks are not the centralized systems. The wireless sensor networks ensure the end-to-end communication between the nodes.

Wireless sensor networks ensure self-healing and self-organizing capabilities. Self-healing permits the sensor nodes to reconfigure themselves and try to find an alternate path for the nodes when the link fails or powered-down. The sensor node gathers and forwards the data to the information sink using the multi-hop wireless network.

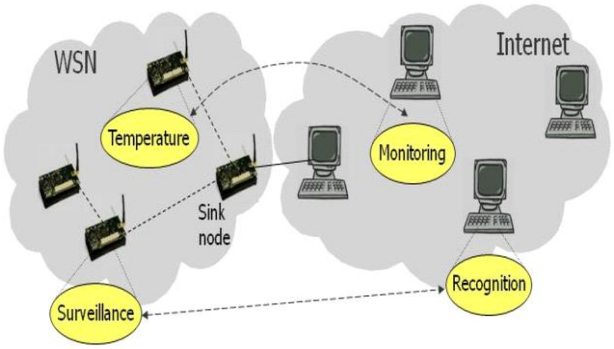

Figure1. WSN's architecture

A sensor network is self-organizing because it allows the network to join a new node without any transmission interfering. Sensors are the powerful devices which are capable of collecting the data from different devices, stores, sensing and conveying the information to the sink or the base station. The sensor networks must have the ability to resist environmental circumstances and it has the ability to cope with the node breakdown. In wireless sensor networks, the sensor nodes are supportive in nature and are organized in a supportive manner. There are no requirements to install, as they can be easily employed anywhere in the network. The data collected from different devices can be retrieved from either the sink or the base station.

The security in wireless sensor networks (WSNs) is a serious concern due to the inherent limitations of computational capability and power usage. Though a variety of security methods are being developed and a lot of research is going on for security concerns at a brisk pace but the field lacks a common integrated platform which provides a wide-ranging

comparison of the apparently unrelated but linked issue user we attempt to relatively analyze the various available security methods highlighting their advantages and limitations. This will surely ease the implementers' burden of choosing between various available modes of defense.

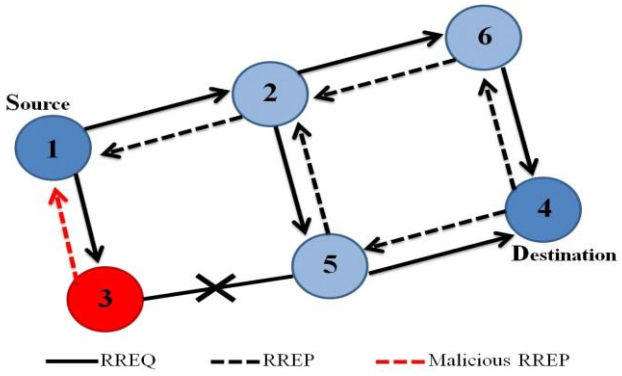

Figure 2: Black Hole Attack Detection

Security permits WSNs to be used with self-assurance and keeps integrity of data. Without security, the use of WSN is any application domain would result in unwanted significances. Particularly in military based projects where a compromise in security cans indication to terrible significances. Thus security must be addressed in such critical sensor applications. It tries out that providing security in wireless sensor networks is pivotal due to the fact that resources such as power, bandwidth, computation, and storage inherently limit sensor nodes.

2. PREVIOUS STUDY

A black hole threat means that one malicious node manipulates the routing protocol to claim itself of existence the shortest path to the destination node, but drops the routing data but does not forward packets to its neighbors. A solo black hole attack is easily occurs in the WSN.

A.Babu Karuppiah et al. have proposed an improvised hierarchical vitality efficient intrusion detection system is proposed, to protect sensor Network from black hole attacks. Previous approach is simple and is based on exchange of control packets between sensor node and base station. The results show that our proposed algorithm is effective in detecting and preventing competently the black hole attacks.

Rakesh Kumar Gautam et al. Authors have presented some black hole attack detection and prevention methods researched by the authors. Most of the attacks beside security in wireless sensor networks are affected by the addition of wrong information by the compromised nodes in the network. On behalf of defending the inclusion of false reports by compromised nodes, a means is mandatory for identifying false reports. Though, building such a detection method and making it efficient represents a great investigation task. Again, confirming complete security in wireless sensor network is a major research issue. Most of the proposed security schemes are based on specific network models. In this paper we summarized various black hole detection and prevention technique.

Karishma Chugh et al. Authors have studied the malicious nodes, which continue to send self-generated data packets cause an increase in the number of DIO messages exchanged between nodes while malicious nodes, which suppress self-generated data packets are able to disguise the instability of network by having no effect on the number of DIO messages or packet delay. Scenario with malicious node sending self-generated data packets showed 8% increase in total number of DIO packets exchanged amongst nodes while scenario with malicious node not generating any data packets had less number of DIO messages exchanged thus falsely presenting a stable network topology. It was also found that data packets suffer delay in presence of malicious activity in the network. Data packets generated by malicious nodes were 4.3 times higher delayed as compared to data packets from their counterparts in clear network. Data packets from non-malicious nodes also suffered considerably higher delay. Thus, increased packet delay and increase in exchange of DIO messages can be treated as preliminary indicators of malicious activity but more concrete parameters are required to identify malicious nodes. This case study may be helpful in designing an effective defense system against known attacks on wireless sensor networks.

Nadeem Ahmed et al. Authors have given the details of different types of holes, discuss their characteristics and study their results on successful working of a sensor network. We present advanced in research for addressing the security threats related difficulties in wireless sensor networks and discuss the comparative concentrations and limitations of the proposed solutions for combating different kinds of holes.

3. PROBLEM FORMULATION

No attention has been given to the detail to study the effect of Black Hole attack in WSN using Reactive and Hybrid routing protocols and to compare the vulnerability of both these protocols against the attack. There is a need to address these kinds of protocols underneath the attack, as well as the impacts of the attacks on WSN. Proposed study analyzes Black Hole attack in WSN using reserve path based node activity and link health tracking for the detection and elimination the black hole nodes.

4. METHODOLOGY

This research will start with previous study of existing WSN routing protocol's performance against black hole attacks. In the literature study, we will study the existing WSN routing algorithms. Previous study will lead towards the implementation of all of the above-mentioned WSN routing protocols in NS2. It also becomes quite important to conduct a

detailed review about the performance analyzing parameters. The Simulation will be done in NS2. A detailed performance and feature-testing system would be designed and developed to analyze the performance of the WSN ROUTING PROTOCOLS (AODV, TORA and DSR) under Black hole attack.

5. CONCLUSION

With this study, the black-hole attacks can detect easily. And with prevention from these attacks the communication will never break in WSN. With RPB approach there will be reserve paths to continue the communication if black-hole finds in the existing path.

REFERENCES

[1] Karuppiah, A. Babu, et al. "An improvised hierarchical black hole detection algorithm in Wireless Sensor Networks." *Innovation Information in Computing Technologies (ICIICT), 2015 International Conference on*. IEEE, 2015.

[2] Jangra, Dr Banta Singh, and Vijeta Kumavat. "A Survey on Security Mechanisms and Attacks in Wireless Sensor Network." *International Journal of Engineering and Innovative Technology (IJEIT)* 2.3 (2012): 291-296.

[3] Le, Anhtuan, et al. "6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach." *International Journal of Communication Systems* 25.9 (2012): 1189-1212.

[4] Ahmed, Nadeem, Salil S. Kanhere, and Sanjay Jha. "The holes problem in wireless sensor networks: a survey." *ACM SIGMOBILE Mobile Computing and Communications Review* 9.2 (2005): 4-18.

[5] Sharma, Preeti, Monika Saluja, and Krishan Kumar Saluja. "Detection techniques of selective forwarding attacks in wireless sensor networks: a survey." *arXiv preprint arXiv:1205.4905* (2012).

[6] Priya, Anu, and Amit Puri. "REMOVAL OF SELECTIVE BLACK HOLE ATTACK WITH UPSTREAM NODE AND DOWNSTREAM NODE ALARM SYSTEM BY DYNAMIC SOURCE PROTOCOL (DSR)." *Int J Adv Engg Tech/Vol. VI/Issue IV/Oct.-Dec* 3 (2015): 07.

[7] Gondwal, Nitesh, and Chander Diwaker. "Detecting blackhole attack in WSN by check agent using multiple base stations." *American International Journal of Research in Science, Technology, Engineering & Mathematics* 3.2 (2013): 149-152.

[8] Kaur, Rupinder, and Parminder Singh. "Review of black hole and grey hole attack." *The International Journal of Multimedia & Its Applications* 6.6 (2014): 35.

[9] Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao. "A survey of black hole attacks in wireless mobile ad hoc networks." *Human-centric Computing and Information Sciences* 1.1 (2011): 1-16.

[10] Pathak, Ganesh R., Suhas H. Patil, and Jyoti S. Tryambake. "Efficient and trust based black hole attack detection and prevention in WSN." *International Journal of Computer Science and Business Informatics* 14.2 (2014).

[11] Songqiao Han, Yong Zhang , "*Design and Implementation of Service Composition Protocol Based on DSR*", in proceedings of The 11th International Conference on Parallel and Distributed Computing, Applications and Technologies, 2010.

[12] Yogesh Chaba, Yudhvir Singh , Manish Joon, " *Simulation Based Performance Analysis of On-Demand Routing Protocols in MANETs*", in proceedings of The Second International Conference on Computer Modeling and Simulation, 2010