IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

A Proposal for Detecting Vampire Attacks in Wireless Sensor Networks

Shiwani N. Laghawe[1], Nekita A. Chavan[2]

PG Student, Department of Computer Science, G.H. Raisoni College of Engineering, Nagpur, India [1]

Professor, Department of Information Technology, G.H. Raisoni College of Engineering, Nagpur, India [2]

Abstract: Wireless sensor networks (WSNs) are the foremost promising research direction in sensing and pervasive computing. Previous security work has focused totally on denial of service at the routing or medium access management levels. Earlier, the resource depletion attacks are thought about solely as a routing drawback, very recently these are classified into new category as "vampire attacks". Planned work examines the resource depletion attacks at the routing protocol layer that disable networks permanently by quickly debilitating node's battery power. The new method for detecting Vampire Attacks is discussed in this paper.

Keywords: Network Lifetime, Routing Protocols, Vampire Attack, Wireless Sensor Networks.

I. INTRODUCTION

A wireless sensor network contains number of sensors that are distributed across a wide geographical area. Several applications uses a constitute network which is formed by autonomous sensor [1]. The applications are structural health monitoring, health-care monitoring, industrial monitoring, instantly deployable communication for military, on-demand computing, inventory tracking, power management, factory performance, power, smart sensing thereby information or data gathering and processing, seismic detection and acoustic detection[2].The life of network plays a crucial role in such applications. Many researches focus on increasing the lifespan of WSN [3].

One new type of resource (energy) depletion attack is known as vampire attack [5] which exhausts the battery power of the node to disable the whole network. An adversary compromised the vampire node in sensor network. This node continuously sends messages to other nodes so each node in the network loses energy faster causing the failure of the whole network soon. The vampire attack can target any routing protocol and does not specific to particular protocol. They are difficult to detect because they do not alter the original message.

There are two types of vampire attacks stated in [5] Carousel attack and Stretch attack. In carousel attack a series of loop is formed between the source and the sink node. So the route length is increased and goes beyond the limit of nodes in the network. Due to this energy consumption of nodes increases and thus minimizes the network lifetime. In stretch attack, artificially long route from source to sink is made by an adversary causing packets to traverse a larger route and draining extra energy.

The rest of the paper is categorized as follows. Section II explains Related work. Section III defines the Proposed system. In Section IV Experimental results are discussed. In Section V concludes the paper. Section VI determines the Future scope.

II. RELATED WORK

In 2013 Eugene Y. Vasserman and Nicholas Hopper [5] introduced a definition for vampire attacks. The authors introduced PLGPa protocol which tries to overcome the damage from Vampire attacks. But during the topology discovery phase satisfactory solution for Vampire attacks is not offered and further modifications to PLGPa are suggested. In 2014 Sunil Bhutada, Kranthi Kumar.K, Manisha.K [6] proposed a system which mitigates the vampire attacks by saving bandwidth, power and time. At each node to detect the presence of vampire attacks, route validation will be checked and if present avoids it immediately. Clean-Slate Sensor Network Routing is used to forward the data packets safely. In 2014 Mrs. R.Abirami, and Mrs.G. Premalatha [7] proposed some defenses against vampire attacks and described Interior Gateway Routing Protocol (IGRP) protocol which is a Cisco-proprietary Distance-Vector protocol. This protocol provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destination. Also in 2014 Divya and Vanitha [8] introduced a valuable secure protocol to prevent attacks in wireless ad hoc sensor networks. The network configuration, key management and communication phase are the three phases of VSP. Elliptic Curve Cryptography (ECC) approach is used with VSP. E. Mariyappan and Mr. C. Balakrishnan [9] proposed A Sensor Network Encryption Protocol using boundary recognition technique, recursive grouping algorithm and jump point algorithm so that the correct path is produced to prevent the vampire attacks in forwarding phase. Damodhar and Umakant [10] described the Energy Weighted Monitoring Algorithm to overcome from resource consumption attack. For consuming the nodes energy, two phases are initialized in EWMA. According to simulation results the proposed technique performs well. Sivakumar and Murugapriya [11] described Optimal Energy Boost-up protocol for providing the security. It was found that the energy of network based on the location is increased in forwarding phase. In 2014 Soram rakesh singh and

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Narendra [12] presented MDSDV protocol. M-DSDV protocol is designed to combat the routing loop problems. It was observed that, this system has reduced the damage from vampire attacks in forwarding phase. José Anand and Sivachandar [13] presented the vampire attacks detection in wireless sensor networks. The effect of vampire attacks on AODV is proposed for providing the security. During the forwarding phase, energy of the network is increased. In 2015 Lina R. Deshmukh, and A. D. Potgantwar [14], proposed No-Backtracking property scheme to achieve high efficiency and secure authentication. Within the network by using group identification method the nearest neighbour node is identified. The PLGP protocol is a slate secure routing protocol, which is used to prevent vampire attack during packet forwarding.

III. PROPOSED METHODOLOGY

From the review of security techniques, it is observed that most of the security techniques provide solution in packet forwarding phase only. Proposed Enhanced PLGPa is planned to be at the deficiencies of PLGPa. The proposed work mainly focused on avoiding vampire attacks in the discovery phase of PLGP. A malicious node (vampire) would send high energy signal and usage the packet flooding and RREQ flooding to establish the malicious connection. For trusted nodes estimation signal strength of the group joining messages is checked for each node. In order to provide solution during discovery phase the threshold concept is utilized. This threshold value is used to determine the suspicious node.

$$Threshold = \sum_{i=1}^{N} \frac{number\ of\ broadcast}{N}$$

Now the broadcast values of nodes are compared to the estimated threshold value. The nodes will be divided into two groups such as suspicious node or normal node.

ALGORITHM

1. Start
2. Nodes broadcast the group joining request.
3. Signal Strength of each node will be calculated.
4. Mean threshold value will be calculated.
5. Attackers are started through network
6. PLGPa process started
7. If (signal strength of node < Mean Threshold)
8. Allow the connection to neighboring node.
9. Else
10. Mark node as vampire node and removed from network.
11. Start communication between source and destination.
12. End if
13. End

IV. SIMULATION AND RESULTS

Simulation is done on NS 2.35. Sensor network with 50 nodes is created. Normal communication between nodes, sink nodes and base station takes place.

Figure 1 shows network set up and communication.

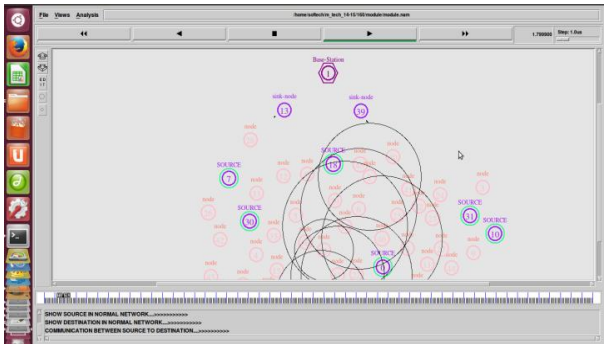

Fig 1: Wireless Sensor Networks and Communication between nodes.

The carousel attack is carried on wireless sensor networks shown in figure 2. In this type of attack a series of loop is formed between the source and the sink node. So the route length is increased and goes beyond the limit of nodes in the network. Due to this energy consumption of nodes increases and thus minimizes the network lifetime. By a factor of O(λ) energy usage increases, where the maximum route length is λ. Energy consumption during attack is measured.

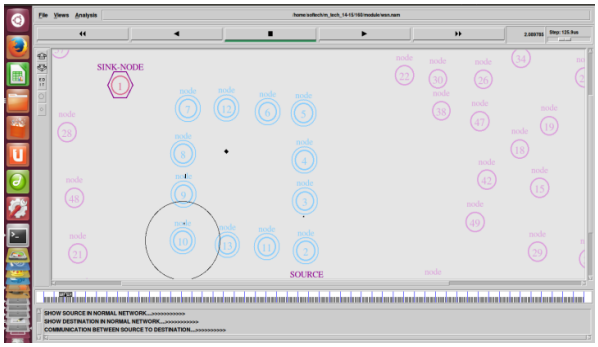

Fig 2: Carousel Attack.

The stretch attack is carried on wireless sensor networks shown in figure 3. In this type of attack artificially a long route from source to sink is made by an adversary causing packets to traverse a larger route and draining extra energy. This attack causes a node that doesn't lie on optimal path to process packets. By a factor of O(min(N, λ)), where the number of nodes in the network is N and the maximum path length is λ. Energy consumption during attack is measured.

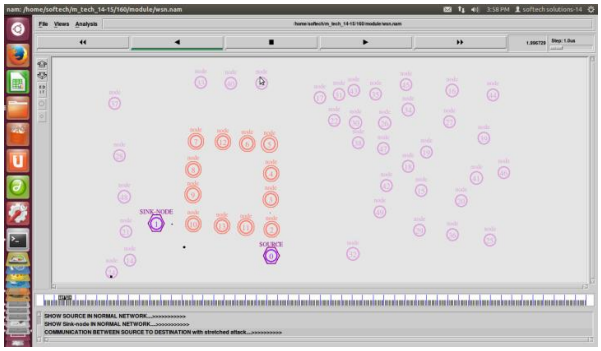

Fig 3: Stretch Attack.

Figure 4 shows Energy consumption during carousel attack is much more than during stretch attack.

DOI 10.17148/IJARCCE.2016.53155

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

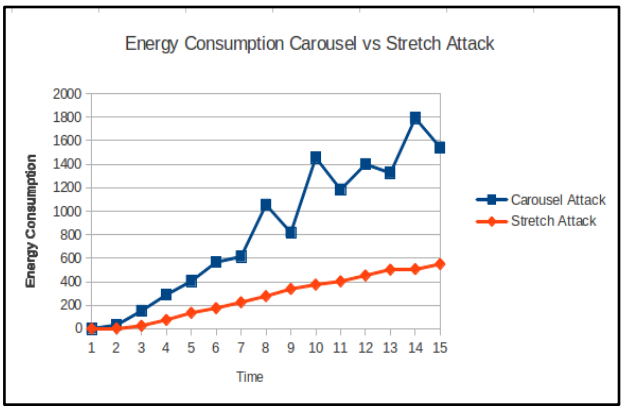

Fig 4: Energy consumption during carousel attack and stretch attack.

V. CONCLUSION

Simulation is done on NS2.35 simulator. A network of 50 nodes is created. Effect of Vampire attack is on network is measured. Energy consumption during carousel attack and stretch attack is determined. Proposed system detects suspicious node which causes vampire attack in the network. Prevention of vampire attack and comparison proposed work with existing work is left for future work.

REFERENCES

[1] Th. Arampatzis, J. Lygeros, S. Manesis "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks", Proceedings of the 13th Mediterranean Conference on Control and Automation Limassol, Cyprus, June 27-29, 2005.

[2] Murtadha M. N. Aldeer, "A Summary Survey on Recent Applications of Wireless Sensor Networks", 2013 IEEE Student Conference on Research and Development (SCOReD), 16 -17 December 2013, Putrajaya, Malaysia.

[3] Long Zhaohua, Gao Mingjun, "Survey On Network Lifetime Research For Wireless Sensor Networks", Proceedings of IC-BNMT2009.

[4] Jyoti Kumari, Prachi, "A Comprehensive Survey of Routing Protocols in Wireless Sensor Networks", 2015 IEEE Conference.

[5] Eugene Y. Vasserman, Nicholas Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", IEEE transactions on mobile computing, VOL. 12, NO. 2, February 2013.

[6] Sunil Bhutada, Kranthi Kumar.K, Manisha.K, "A Novel Approach for Secure Routing Protocol: To Improve Life of Network", 2014 IEEE Conference.

[7] Mrs. R. Abirami, Mrs. G. Premalatha, "Depletion of Vampire Attacks in Medium Access Control Level using Interior Gateway Routing Protocol", ICICES2014 - S. A. Engineering College, Chennai, Tamil Nadu, India.

[8] K. Vanitha, V. Divya, "A Valuable Secure Protocol to Prevent Vampire Attacks in Wireless Ad Hoc Sensor Networks" International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 3, 2014.

[9] E. Mariyappan, Mr. C. Balakrishnan, "Power Draining Prevention In Ad-Hoc Sensor Networks Using Sensor Network Encryption Protocol", ICICES2014 - S. A. Engineering College, Chennai, Tamil Nadu, India.

[10] B. Umakanth, J. Damodar , "Resource Consumption Attacks in Wireless Ad Hoc Sensor Networks" international Journal of Engineering Research Volume No.3 Issue No: Special 2, pp: 107-111, 2014.

[11] K. Sivakumar, et.al, "Efficient Detection and Elimination of Vampire Attacks in Wireless Ad-Hoc Sensor Networks" International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, 2014.

[12] Soram Rakesh Singh, Narendra Babu C. R, "Improving the performance of energy attack detection in wireless sensor network by secure forwarding mechanism" International Journal of Scientific and Research Publications, Volume 4, Issue 7, 2014.

[13] Jose Anand, K. Sivachandar, "Vampire Attack Detection in Wireless Sensor Network" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 4, 2014.

[14] Lina R. Deshmukh, A. D. Potgantwar, "Ensuring an Early Recognition and Avoidance of the Vampire Attacks in WSN using Routing Loops", 2015 IEEE International Advance Computing Conference (IACC).

BIOGRAPHY

Shiwani Laghawe received the bachelor's degree in Computer science and engineering from the Nagpur University, Maharashtra, India in 2013. Presently she is pursuing her master's in mobile technology in the department of Computer Science from G. H. Raisoni College of Engineering, Nagpur Maharashtra, India. Her research interests include wireless sensor networks, cryptography and network security, wireless security etc.

DOI 10.17148/IJARCCE.2016.53155