ISSN: 2456 - 3935

International Journal of Advances in Computer and Electronics Engineering
Volume: 02 Issue: 02, February 2017, pp. 13 – 16

Strategies for Detection and Prevention of Vampire Attack in WSN

Vikas Juneja
Assistant Professor, Department of Information Technology
Jai Parkash Mukand Lal Institute of Engineering and Technology (JMIT), Radaur, India
Email: vikasjuneja2002@gmail.com

Dr. D.V. Gupta
Professor, College of Engineering Roorkee (COER), Roorkee, India
Email: dvgupta.rke@gmail.com

Abstract: *Wireless Sensor Network (WSN) is a wireless network consisting of autonomous nodes spatially distributed using sensors to monitor environmental or physical conditions. These intermediate nodes may cause network so security in WSN is a very difficult task. In this paper vampire attack and its various detection techniques are presented with literature review of different research papers that covers detection and prevention mechanism of Vampire attacks. In WSN, Energy is an important factor for sensor node. There is one new type of attack called vampire attack which disables network by crushing battery life of sensor nodes in a network. So it is difficult to find vampire attack and prevent network from them. These techniques are used in the prevention of network from vampire attack.*

Keyword: *WSN; Security; Vampire Attack; Denial of service; Carousel attack;*

1. INTRODUCTION

The production of low prize and small size sensor nodes became economically and technically feasible due to recent technical advancement. A Wireless Sensor Network is composed of number of these sensor nodes may be in thousands. Information between these sensor nodes can be transferred inside the network or directly to an outer base-station node. Sensor nodes transfer sensed data to each other and form high-quality useful information about the surrounding environment. Various application areas of these nodes are such as in monitoring various environmental conditions, in military communication services.

For these applications, these sensor nodes should be more reliable and compatible. For performing any communication or transfer message, these nodes require the power from its battery. Network performance can be degrade if the node uses more battery power for its work then its lifetime is less and that node can disconnected from the networks. The wireless sensor network is ad-hoc in nature so it is vulnerable to Denial of service attack [1]. Denial of service (DOS) attack is an attempt to make a machine or network resource unavailable to its intended users.

Jamming the signal, power exhaustion and flooding with useless traffic are various types of DOS attack. In power exhaustion, adversary attacks on the nodes and consumes more battery power of the node [2]. Vampire attack is also the type of power exhaustion attack.

1.1 Challenges in WSN

Various challenges are discussed in this section that is occurred during data transmission in WSN. These are as follows:

(i) Node-to-node communication and acknowledgement: With a specific end goal to send the information from source to destination, the node can hold up till it experiences the destination node and after that send the message to the destination straightforwardly.

(ii) Node-Network Capacity: For deciding the measure of information that can be conveyed, likewise limit of basic system is a critical element. Different nodes tries to forward information, the system may get to be congested. Accordingly, this element record out that if a message should be divided or not with a specific end goal to send it from source to the destination.

(iii) Storage Capacity: The capacity limit of nodes is confined. The nodes attempt to swap every one of the information what they right now keep with them. In this manner, if the nodes have capacity appreciative the node supports will flood and it will come about into message adversity [3].

1.2 WSN Routing Protocols

A routing protocol is adaptive if some of the network parameters can be adjusted according with the current network state and energy capacity of network nodes. WSN protocols can be classified on the basis of route discovery process from source to destination which are called as reactive, proactive and hybrid routing. On demand route discovery method is used in reactive protocol.

Routes are pre-discovered irrespective to time of sending message in pro-active routing. Mixed of these two strategies are called Hybrid routing protocols. Generally routing protocols in WSN can also be categorized into three categories based on network structure flat-based routing, hierarchical routing and location based routing (Jamal N. Et al., [4]).In Flat-based routing all network nodes poses similar functionalities and equal roles while in hierarchical based routing node acting dissimilar roles assign to them. In case of location-based routing position of sensor nodes are exploited for routing data in the network. Many other protocols are there based on position and timing information.

1.3 Vampire Attack

Vampire attack disable network by draining energy of network nodes [1]. Like an Honest node, Vampire attack causes generating and flooding of messages and drains the battery life from network nodes. Basically vampire attack is a type of Distributed DOS (DDOS) attack, which performs resources consumption on neighbor nodes. In Vampire attacks, targeted packets are modified by misguiding the packets or by preparing long routes. Using false control message exchange, malicious nodes make frequent connectivity from the entire neighbor nodes in network .Due to these false control messages, neighbor nodes replies the false request for connectivity and draining energy rapidly. It is very difficult to detect the attack as the malicious host only changes little information of the packets. Vampire attack represent of many attacks [1]. They’re as follows:

Directional antenna attack: Directional antenna attack is the main reason behind vampire attack. Vampires have very little management over packet progress once forwarding choices are made severally by every node; however they'll still waste energy by restarting a packet in varied parts of the network. There are two forms of vampire attacks supported this directional antenna attack. They’re Stretch attack and carousel attack.

Carousel attack: In carousel attack, associate degree adversary composes packets with intentionally introduced routing loops. It targets supply routing protocols by exploiting the restricted verification of message headers at forwarding nodes, permitting one packet to repeatedly traverse identical set of nodes.

Stretch attack: In Stretch attack, associate degree resister constructs unnaturally long routes, potentially traversing each node within the network. It will increase packet path lengths; inflicting packets to be processed by form of nodes that's freelance of hop calculate the shortest path between the resister and packet destination.

Malicious discovery attack: Another attack on all previously-mentioned routing protocols (including stateful and stateless) is spurious route discovery. In most protocols, each node can forward route discovery packets and generally route responses as well, that means it's potential to initiate a flood by causation one message.

2. LITERATURE REVIEW

Eugene Y. Vassermann and Nicholas Hopper [1] described clean-slate secure sensor routing protocol by Parno, Luk, Gaustad, and Perrig (PLGP) & PLGP with attestations (PLGP-a). In this, PLGP protocol is used. The path tracking technique is used in PLGP to securely transmit the data. No-Backtracking property is suggested to achieve high efficiency and secure authentication .But PLGP does not satisfy the no-backtracking property. So authors described PLGP-a method which satisfies the no-backtracking property. Disadvantage of this projected work is limited to packet forwarding phase only. This solution does not work in topology discovery phase.

B. Umakanth and J. Damodhar [5] described the detection on Energy draining attack using Energy Weighted Monitoring Algorithm (EWMA) in wireless ad hoc sensor networks. It was described the resource consumption attacks in wireless ad hoc sensor networks. EWMA algorithm has two phases like network configuration and communication phase. Implementation was done using small number of nodes. Network configuration phase used to establish an optimal routing path from source to destination. Communication phase avoids the same data packets and aggregated the data transmission.

Priyanka P. Pawar and Shailaja N. Uke [6] presented a technique called DLWASN (name of protocol) in which secure hash function is used as cryptographic function. In this presented routing algorithm, results were computed based on four parameters like packet drop ratio (PDR), energy, throughput and delay. Disadvantage of this described solution is that while considering PDR, energy consumption and throughput, protocol gives better results than the others but packet transmission delay is not better in this algorithm.

K. Vanitha, and V. Dhivya[7] explained Valuable secure protocol (VSP) & Elliptic Curve Cryptography (ECC) algorithms. In this presented technique, Modification of Clean slate sensor routing protocol was done. It has three phases like network configuration phase, key management and communication phase. The key management phase is used for cryptography to protect the node and data. ECC approach is used to achieve the security with smaller key size.

Jose Anand, and K. Sivachandar [8] presented the effect of vampire attacks on Adhoc on-demand vector (AODV) routing protocol for providing the security. Rivest, Shamir, Adleman (RSA) algorithm is used for providing the security. Randomly selected malicious AODV agents are evaluated. Initial energy and final energy are used to calculate the energy level in the networks.

Ankita Shrivastava and Rakesh Verma [9] discussed packet monitoring technique. The basic principle behind the approach is that nodes check the received route request by comparing the packet header’s information like broadcast id and destination address during route discovery phase and discard the malicious packets. Performance of mentioned approach decreases as the number of nodes increases in the network.

Ashish Patil and Rahul Gaikward [10] explained Trust model in which three steps were used to prevent vampire attack. First, reduce the impact of Carousel attack; second, reduce the impact of Stretch attack and third, perform secure routing based on trust value. Trust value of each node can be calculated by calculating: The total packets they transmit, Total packets they receive, Total packets they drop. Attacker node which is having low trust value is eliminated from transmission. Disadvantage of this algorithm is that full satisfactory solution has not offered for vampire attacks.

Soni & Pahadiya B. [11] described a new methodology based on energy threshold and packet broadcast threshold of sensor node of network. There was the dynamic detection of removal of vampire attack. This solution is simple and also works with topology change in network.

G. Lakshmi Narayana and Koteswara Rao [12] discussed the Computed Energy level of the nodes. Discussed algorithm computed the influence of the attack by the ratio of network energy used in compassionate case to the energy used in the malicious case i.e. the relation of network-wide power operation with malicious nodes present to energy process with only honest nodes when the number and size of packets sent remains steady.

3. EXISTING TECHNIQUES

PLGP: The path tracking technique is used in PLGP to securely transmit the data. No-Backtracking property is suggested to achieve high efficiency and secure authentication. But PLGP does not satisfy the no-backtracking property.

PLGP with attestations: PLGP-a method which satisfies the no-backtracking property. Disadvantage of this presented work is limited to packet forwarding phase only. This solution does not work in topology discovery phase.

EWMA: Detection of Vampire attacks using Energy Weighted Monitoring Algorithm in wireless ad hoc sensor networks. EWMA algorithm has two phases like network configuration and communication phase. Network configuration phase used to establish an optimal routing path from source to destination. Communication phase avoids the same data packets and aggregated the data transmission.

ECC: Elliptic Curve Cryptography approach is used to achieve the security with smaller key size. It is the modification of clean slate sensor routing protocol. It has three phases like network configuration phase, key management and communication phase. The key management phase is used for cryptography to protect the node and data.

AODV using RSA: RSA cryptographic technique is used to detect the effect of vampire attacks on AODV.RSA algorithm is used for providing the security. Randomly selected malicious AODV agents are evaluated. Initial energy and final energy are used to calculate the energy level in the networks.

Packet monitoring: basic principle behind the approach is that nodes check the received route request by comparing the packet header’s information like broadcast id and destination address during route discovery phase and discard the malicious packets. Performance of mentioned approach decreases as the number of nodes increases in the network.

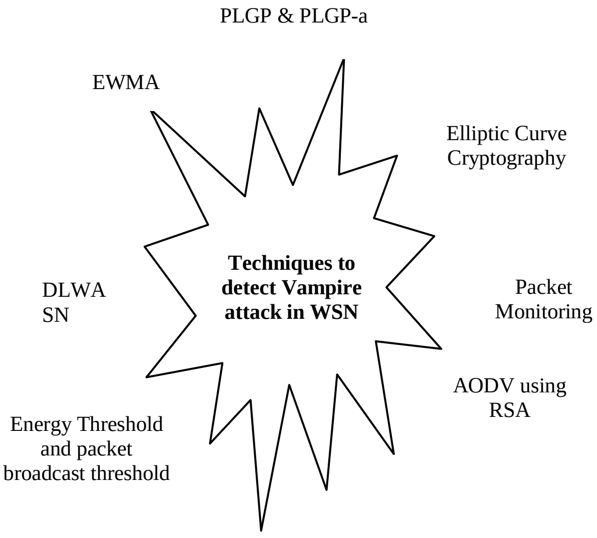
PLGP & PLGP-a
EWMA
Elliptic Curve Cryptography
Techniques to detect Vampire attack in WSN
DLWA SN
Packet Monitoring
AODV using RSA
Energy Threshold and packet broadcast threshold

Figure 1 Techniques - detection of Vampire attack

Energy and packet broadcast threshold: new methodology based on energy threshold and packet broadcast threshold of sensor node of network. There was the dynamic detection of removal of vampire attack. The presented solution is simple and also works with topology change in network.

4. CONCLUSION AND FUTURE WORK

In this paper WSN and its various challenges, and its routing protocols are presented. Vampire attack and its requirements are also discussed. After that detailed review of Vampire attack detection techniques has been provided with their pros and cons. In future it is intended to propose a new methodology that detects vampire nodes and prevent network from vampire attack.

REFERENCES

[1] Eugene Y. Vassermann and Nicholas Hopper, (2013), "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", IEEE Trans. Mobile Computing, vol. 12, no. 2, pp. 318-332.

[2] Ashish Patil and Rahul Gaikwad, (2015) "Comparative analysis of the prevention techniques of denial of service attacks in Wireless Sensor Networks", Procedia Computer Science, Vol 48, pp. 387 – 393.

[3] Maurice J. Khabbaz, Chadi M. Assi and Wissam F. Fawaz,(2012), "Disruption-Tolerant Networking. A Comprehensive Survey on Recent Developments and Persisting Challenges", IEEE Communications Surveys & Tutorials, Vol. 14,No.2.

[4] Jamal N. Al-Karaki Ahmed E. Kamal, Routing Techniques in Wireless Sensor Networks: A Survey.

[5] B. Umakanth and J.Damodhar,(2013), "Detection on Energy draining attack using EWMA in wireless ad hoc sensor networks", International Journal of Engineering Trends and Technology, Volume 4, Issue 8.

[6] Priyanka P. Pawar and Shailaja N. Uke, (2014), "Vampire attack detection and prevention using DLWASN on wireless adhoc sensor network", International Journal of Research in Computer Science**,** Volume 01, Issue 03.

[7] K.Vanitha, and V.Dhivya,(2014), "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 03, Special Issue 03.

[8] Jose Anand, and K. Sivachandar, (2014), "Vampire Attack Detection in Wireless Sensor Network", International Journal of Engineering Science and Innovative Technology, Volume 03, Issue 04.

[9] Ankita Shrivastava and Rakesh Verma, (2015) ,"Detection of Vampire Attack in Wireless Ad-hoc Network", International Journal of Software & Hardware Research in Engineering, Volume 03, Issue 01.

[10] Ashish Patil and Rahul Gaikward,(2015), "Preventing vampire attack in wireless sensor network by using trust model," International Journal of Engineering Research & Technology, Volume 4,Issue 06.

[11] Soni & Pahadiya B.,(2015), "Detection and Removal of Vampire Attack in Wireless Sensor Network", International Journal of Computer Applications, Volume 126, Issue 07.

[12] G.Lakshmi Narayana and Koteswara Rao,(2015), "A Sensor Network Routing Protocol To Clear The Damage From Vampire Attacks During Packet Forwarding", International Journal of Science Engineering and Advance Technology, Volume 03, Issue 01.

Author Biography

Vikas Juneja is an Assistant Professor, of Department of Information Technology in JMIT, Radaur (Distt. Yamunanagar) Haryana. He completed his M.E. in CSE at NITTTR, Chandigarh. His area of interest includes in Cryptography and Network Security.