International Journals of Advanced Research in Computer Science and Software Engineering
ISSN: 2277-128X (Volume-7, Issue-8)

Research Article | **August 2017**

Impact of Vampire Attack on Performance of Wireless Sensor Networks: A Survey

Taruna Malviya
M.tech Student, Jagadguru Dattatray College of Technology, Indore, Madhya Pradesh, India

Khushboo Sawant
Assistant Professor, Jagadguru Dattatray College of Technology, Indore, Madhya Pradesh, India

DOI: 10.23956/ijarcsse/V7I8/0116

Abstract— A wireless sensor networks is a temporary, infrastructure less network where nodes communicate without any centralized mechanism. This dynamic behaviour of WSN makes this network more potentially applicable in conference, battlefield environment and disaster relief, and has received significant attention in recent years. Attacker may use this weakness to disrupt the network. Subsequently, Power draining is the major thread; where attacker not only exhausts the network traffic but also degrades the life of node as well network. The objective of this study is to detect and prevent wireless sensor networks from unwanted power draining due to Vampire attack. Here, Targeted Flooding through high battery capacity node has been used to deploy Vampire attack in mobile ad-hoc network. Subsequently, energy consumption and capacity observation technique has been used to detect malicious node(s). Furthermore, prevention method forcefully shutdown malicious nodes and transfer communication.

Keywords— Wireless Sensor Networks, Vampire Attack, AODV

I. INTRODUCTION

A Wireless Sensor Network is usually composed of hundreds or thousands of sensor nodes. These sensor nodes are often densely deployed in a sensor field and have the capability to collect data and route data back to a base station (BS). A sensor consists of four basic parts: a sensing unit, a processing unit, a transceiver unit, and a power unit. It may also have additional application-dependent components such as a location finding system, power generator, and mobilize as shown in Figure 1.1.

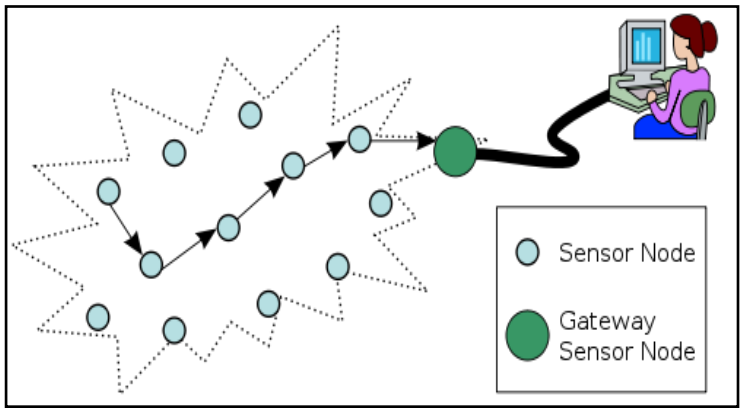

Figure 1: Wireless Sensor Networks

Due to open nature communication medium, it becomes more vulnerable to outside attacks. Security threats are classified in two category passive and active attacks. In passive attack attacker can listen the packets in the network while in the active attack attacker can also modify the packet contents. Subsequently, little attack may lie into both categories. Poor resources availability is the major weakness of wireless Ad-Hoc network. Attacker may use this weakness to disrupt the network. Subsequently, Power draining is the major thread; where attacker not only exhausts the network traffic but also degrades the life of node as well network.

Vampire attack is such kind of attack which aims to disrupt the network by draining resource capability. Here, Attacker communicates worthless messages formally known as false packet to increase network traffic and make target node busy in useless activity.

Vampire attack is energy draining attack where messages send by the malicious node which causes more energy consumption. This energy consumption is very high and leading to slow depletion of network node's battery life. Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance vector, source routing and geographic and beacon routing. Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, so it takes large energy to transmit the data and consumes the node energy. Since Vampires use protocol-compliant messages, and because of this, detection and prevention are very difficult in this attack. Two types of Vampire attack are as follows:

ISSN(E): 2277-128X, ISSN(P): 2277-6451, DOI: **10.23956/ijarcsse/V7I8/0116,** *pp. 96-99*

1.1 Carousel Attack

In the Carousel attack, [4] attackers introduce some packet within a route as a sequence of loops, such that the same node appears in the route of communication many times.

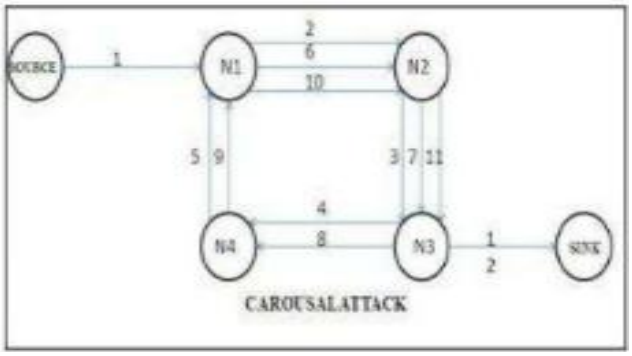

Fig. 1 (a) Carousel Attack

Honest path must be the 1-2-3-12 but in the presence of vampire attack communication path generating loop which is due to the vampire attack and the path is 1-2-3-4-5-6-7-8-9-10-11-12. Node N1, N2, N3, N4 is communication in loop and making carousel attack.

1.2 Stretch Attack

For this type of attack malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. The honest path is very less distant but the malicious path is very long to make more energy consumption.

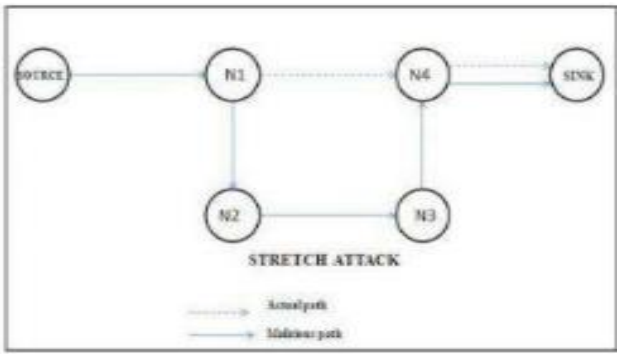

Fig. 1 (b) Stretch Attack

Honest path must be S-N1-N4-D the dotted arrow showing the honest path but the stretch attack generates the long path and it causes more energy consumption.

II. RELATED WORK

To understand the concept and impact of power draining on WSN, work considers certain research work which is explain below:

Zubair A. Baig et. Al [1] proposed a solution where it concludes that Distributed Denial of Service attack is most popular attack for power draining. They also discussed about various attack models and impact. They designed pattern recognition problem to detect DDOS attack. Proposed method improves performance on basis of timely and energy-efficient manner.

Ambili M. A, Biju Balakrishnan [3] proposed energy draining in WSN and introduced energy Based Intrusion Detection System. Intrusion Detection method detect vampire node on the basis of energy level of the node. All node that present in the network will have same energy level and during the communication little changes will take place. Intrusion Detection based on the fact that the malicious node will l have more power than other node because it will consumes other nodes energy so it will aver high energy level. Thus all nodes energy level measured and the node which have abnormally high energy, considered as vampire node.

Chahana B. Thakur , V.B.Vaghe la [4] describe vampire attack and its types and introduced flag based technique to detect and prevent vampire attack. Flag set to header to it cannot take much space and can prevent from the repeated path as for the carousel attack. Flag initializes with 0 and when RREQ generates it set to ne one and when RREP generates it incremented by one so the flag field is key point to discover the basic loop and since vampire attack is to be detected.

Eugene Y. Vasserman et al [5] discovered that every studied protocol is vulnerable to vampire attacks that are complex to discover and simple to introduce with the help of one malicious node transferring. At its worst case, only single attacker is able to enlarge extensive battery power consumption by a factor of O (N), where N is number of nodes in network. Author discusses solution to moderate all vampire attacks that include a fresh proof – of - concept which provably limits the harm caused by attacker in duration of the packet forwarding phase.

III. SECURITY FLAWS

Wireless network is a special network which has many flaws compared to traditional wireless network. Due to these flaws it is very difficult to change the existing security approaches to the area of wireless network. These flaws are

I. Very limited memory and storage space.

A mobile node is a tiny device with small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm.

II. Power limitation.

Energy is the biggest constraint to wireless network. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors). Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network. When implementing a cryptographic function or protocol within a sensor node, the energy impact of the added security code must be considered. When adding security to a sensor node, we are interested in the impact that security has on the lifespan of a sensor (i.e., its battery life). The extra power consumed by sensor nodes due to security is related to the processing required for security functions (e.g., encryption, decryption, signing data, verifying signatures), the energy required to transmit the security related data or overhead (e.g., initialization vectors needed for encryption/decryption), and the energy required to store security parameters in a secure manner (e.g., cryptographic key storage).

III. Unreliable transferring of packets.

Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. Furthermore, the unreliable wireless communication channel also results in damaged packets. Higher channel error rate also forces the software developer to devote resources to error handling. More importantly, if the protocol lacks the appropriate error handling it is possible to lose critical security packets. This may include, for example, a cryptographic key.

IV. Packet Conflicting.

Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network. If packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail. In a crowded (high density) sensor network, this can be a major problem.

IV. PROBLEM STATEMENT

The AODV routing protocol is a popular reactive routing protocol for small scale wireless networks. The major issue with this routing protocol, it is designed for better performance of the network not for security of node, secure protocols are generally designed to have features such as authentication, integrity, confidentiality and non-repudiation. For security purpose AODV have vulnerabilities and it is easily manipulate by malicious node to destroy its network routing.

In order to implement WSN using AODV routing protocol, arrival may use this weakness to disrupt the network by draining resource constraint. Subsequently, DDOS attack is use for intentional power draining. Power draining does not only degrade the node capability but lead to decrease the node life along with network too.

The complete work determine that, there is need to develop a scheme to avoid power draining problem in WSN using AODV to sustain node life and improve the network performance over DDOS attack.

The major problems with AODV are:-

- Zero Security Policy: No Provision to prevent communication form any security Threats.
- Vulnerable for unreliable and discontinuous communication.
- Prone for Disruption of physical network components or worthless resource consumption.
- Attacker may use these vulnerabilities to degrade battery power and lead to reduce node life along with network too.
- Security needs extra Power Utilization.

V. CONCLUSIONS

This research work would carry out the detailed study and analysis of AODV routing protocols and security issues and attacks in WSN theoretically and through simulation. This research work carried out the study of routing protocols and various security threats. This research work proposed IDS based detection technique to identify malicious node(s) into ad-hoc networks. NS-2 simulator has been used to simulate and evaluate the performance of proposed system. Simulation of security strategies provides the facility to select a good security solution for routing protocols and gives the knowledge how to use these schemes in hostile and compromised environments. Energy consumption in the static node scenario and the mobile node scenario is less in compare to vampire attack but high with the compare of original AODV protocol.

REFERENCES

[1] Zubair A. Baig et. “Distributed Denial of Service Attack Detection in Wireless Sensor Networks” Doctor of Philosophy Monash University January, 2008.

[2] "The Network Simulator - ns-2," http://www.isi.edu/nsnam/ns,2012.
[3] Ambili M. A, "Vampire Attack : Detection and Elimination in WSN", in International Journal Of Scientific Research Volume:3 April 2014 ISSN No 2277-8179
[4] Chahana B. Thakur; V.B. Vaghela "Detection and Elimination of Vampire Attack in Mobile Ad hoc Network" Indian Journal of Applied Research Volume: 5 Jan 2015 ISSN No 2249-555X.
[5] T.W. Mehran Abolhasan, "A review of routing protocols for mobile ad hoc network," ELSEVIER, Ad-hoc Network, vol. 2, pp. 1-22, 2004.
[6] M. B. Hardeep Kaur, "Performance of AODV, OLSR AND ZRP Routing Protocol under the blackhole Attack in WSN," IJAREEIE, vol. 2, pp. 2320-3765, June 2013.
[7] V. V. P. Rajipriyadharshini, "Vampire Attacks Deploying Resources in Wireless Sensor Network," International Journal of Computer Science and Information Technology, vol. 5, no. 3, pp. 2951-2953, 2014.
[8] D. J. A. P. Preethi Monoline, "Cache Consistency and IDS for Handling Attacks in Routing Ad-hocNetwork," International journal of Innovative Research in Computer and ommunication Engineering, vol. 2, no. 4, 2007.
[9] S. R. Susan Sharon George, "Attack-Resistant Routing for Wireless A- hoc Network," International Journal of Computer Science and Information Technologies, vol. 5, no. 3, pp. 420- 442, 2014.
[10] I.-R. C. Fenye Bao, "Hierarchical Trust Management for Wireless Sensor Networks and its Application to Trust-Based Routing and Intrusion Detection,"IEEE Transaction on network and service managemnet, vol. 9, no. 2, July 2012.
[11] J. D. B. Umakanth, "Detection of Energy draining attack using EWMA in Wireless Ad-hoc Sensor Network," International Journal of Engineering trends and Technology, vol. 4, no. 8, August 2013.
[12] Y.Yuanming Wu,"Insider Threats against Trust Mechanism with Watchdog and Defending Aproaches in Wireless Sensor Networks," IEEE Symposium on Security and Privacy workshop, 2012.
[13] K. S. Jose Anand, "Vampire Attack Detection in Wireless Sensor Network," International Journal of Engineering Science and Innovative Technology, vol. 3, no. 4, July 2014.
[14] Buchegger, S. and J.-Y.L. Boudec. Cooperative Routing in Mobile Ad-hoc Networks: Current Efforts against Malice and Selfishness. 2002. Springer.
[15] Baker, F., Network Working Group, 2002, Cisco Systems. p. 40.

