A Mitigation Approach to Protect Wireless Sensor Networks over Vampire Attack

Mohit Raikwar
Research Scholar-MTECH
Department of Information Technology,
Vikrant Group of Institutions

Prakash Mishra
Assistant Professor,
Department of Information Technology,
Vikrant Group of Institutions

ABSTRACT

Wireless sensor network is collection of sensor nodes deployed with the aims to sense and process particular attributes. It is kind of wireless network uses radio communication technique for transmission purpose. Sensor nodes integrate several different component such memory, battery, sensor, processing unit etc. Wide range of applications makes it popular among the users and researchers are acquiring it as the research domain. This paper aims to explore the issues in sensor networks and proposed a methodology to overcome the same. Vampire attack is one of severe security threat attacks on the energy of sensor node aims to degrade the life and make it into dying condition. This research paper implements a mechanism to detect and mitigate the impact of sensor networks. The complete solution is implemented using NS-2.35 simulator and evaluated on basis of Throughput and Energy Consumption.

Keywords

Vampire Attack, WSN, AODV

1. INTRODUCTION

Wireless sensor networks are the special type of network. WSN shares the confidential data among sensor nodes in real scenarios, like Military battle field, nuclear power plant, target tracking etc. are the kind of application of wireless sensor network in which each packet contents confidential information. Enemies can misuse the information when they are access the network illegally so network needs some security against the outside attackers. The sensor nodes are resource poor by means of their memory, processing and battery, that's why a sensor node cannot meet the expense of the traditional security systems of computer network. So the security mechanism for a sensor network should be very efficient and robust to acquire by a sensor node without any extra consignment on the node.[1]

WSNs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. These attacks are categorized in previous chapter "security issues in WSN" on the basis of their nature. In these attacks, vampire attack is that kind of attack which occurs in Wireless Sensor Networks (WSN). This section describes about vampire attack and impact of vampire attack on WSN.

The complete work observes that Vampire Attack is energy draining attack where malicious node consumes other nodes energy and downs all the nodes energy. This work observes that attacks can be of two types, a resource depletion attack and a routing disruption attack. [2][3] A routing disruption attack tries to alter the routing path e.g.: Worm hole, Sybil attack, etc. whereas the resource depletion attack only focuses on the battery power and memory. The most permanent DoS attack is to entirely deplete nodes' batteries. [4]

This is an instance of a resource depletion attack, with the battery power as the resource of interest. These attacks are commonly called as "Vampire attacks". 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, these attacks are very difficult to detect and prevent.[5]

Impact of Vampire Attack

a) Vampire attacks are not protocol specific.

b) They don't disrupt immediate availability.

c) Vampires use protocol compliant messages.

d) Transmit little data with largest energy drain.

e) Vampires do not disrupt or alter discovered paths.

The vampire attacks can be classified has two types. There are: one is Carousel attack and other is Stretch attack. This research paper aims to develop a mitigation method to detect and prevent integrated Vampire Attack in Wireless Sensor Networks.

2. PROBLEM DEFINITION

As we know, Wireless Sensor Nodes are resource poor and routing of packets is the most difficult task for a network node. It is required to have an efficient routing technique for a WSN and apart from that, Sensor networks are vulnerable to many attacks as we have discussed in the above section. AODV routing protocol is considered to be most robust and efficient routing protocol, hence widely used for a wireless network. A wireless sensor network also prefers to use the same protocol for routing of packets as its On-Demand nature of route discovery. Though AODV is the most robust routing protocol but there are various problems associated with it. AODV is prone to the well none resource depletion attack which is Vampire Attack.[6]

Vampire attack is very difficult to detect in the network because they do not depend on any particular protocol. In order to implement Vampire attack, attacker either compromised the existing node (Insider) or introduces a malicious node in existing scenario between source and destination (Outsider). Afterwards, it starts flooding of packets with modified header information to create extra load to drain the battery of other nodes.

In AODV, Vampire nodes may replicate the RREQs or generate RREQs for dissimilar destinations unnecessarily, while there is no data to be transmitted on those nodes. And do that repeatedly after expiration of the sequence number for that destination. The Vampire node also broadcast all other packets it receives to drain the battery of other nodes. The Vampire node can also alter the header information of a packet before forwarding it, to increase the load on the receiver nodes. It can be done by replacing a destination address by broadcasting address accordingly. For that, the Vampire node should have the part of the discovered route. It is very difficult to detect that kind of malicious activities. As the Vampire node targets the most critical point of sensor nodes i.e. their batteries, therefore it can damage the whole sensor network. AODV do not have any routine to prevent such kind of resource depletion attacks. So Vampire attacks are very dangerous for a wireless sensor network.

3. METHODOLOGY

The purpose of this study is to deploy vampire attack and develop a technique to detect & prevent vampire attack in the wireless sensor networks. Application of wireless sensor networks such as military battle field is used to transmit the confidential data via wireless medium. Wireless networks are also used in national security applications such as monitoring and tracking the borders, nuclear attacks detection etc. Since all the transmission take place through wireless medium where security risks are major so the security of sensitive information is important part thus the security of data is important aspects.

Although, vampire attack does not lie on the vulnerabilities of routing protocol, it can deploy in any situation without making any changes. There are two types to deploy vampire attack one is known as Carousal Attack and another one is Stretch Attack. Subsequently, it may deploy through two ways; one is external attack using high capabilities node and another is internal attack by compromising the trusted node. A brief description for deployment of vampire attack is explained below;

3.1 External Attack

This kind of attack is deployed from the outside of the networks. It does not require any trusted node to be compromise; instead it deploys heavy capability nodes with extra battery life and transmission power. They use strong transmission power to attract more nodes for communication and enhance the transmission range. Subsequently, they use extra battery power to increase the life of sensor node. Although, basic objective of vampire node is to drain the battery of other nodes by creating overwhelming environment through overloaded packets, they may lose their own life due to overwhelming sending of packets. But the draining at vampire node will be very low due to ignorance of extra processing. Still, a little draining may happened. To avoid the dead end chances they use extra battery life by increasing the battery capacity of attacking node. Attacker node consist the double of battery capacity to get extra node life.

3.2 Internal Attack

This is known as attack through trusted node or own node. It is usually deployed within network range and use trusted node by modifying the routing protocols. It may be very dangerous because of generic attacking technique. Although, external node can be observed or discovered through special characteristics but internal attacker node can’t. They follow similar characteristics with genuine node and have same appearance. They obtain same battery life, transmission power, antenna height etc. at the time of deployment. Due to such properties internal attacks are more severe then external attack for detection and prevention.

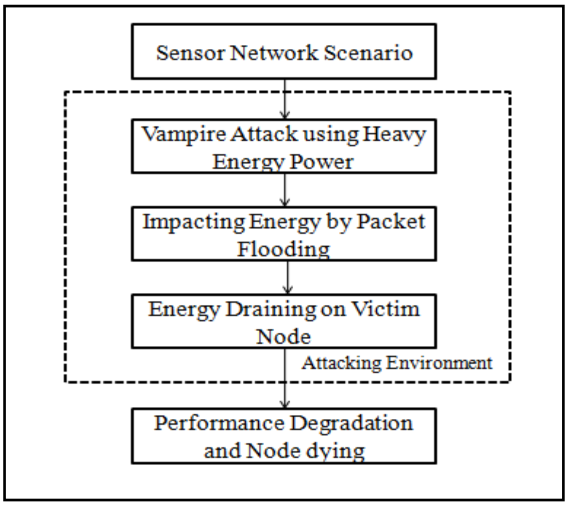
Sensor Network Scenario
Vampire Attack using Heavy Energy Power
Impacting Energy by Packet Flooding
Energy Draining on Victim Node
Attacking Environment
Performance Degradation and Node dying

Figure 3.a: Deployment of Vampire Attack

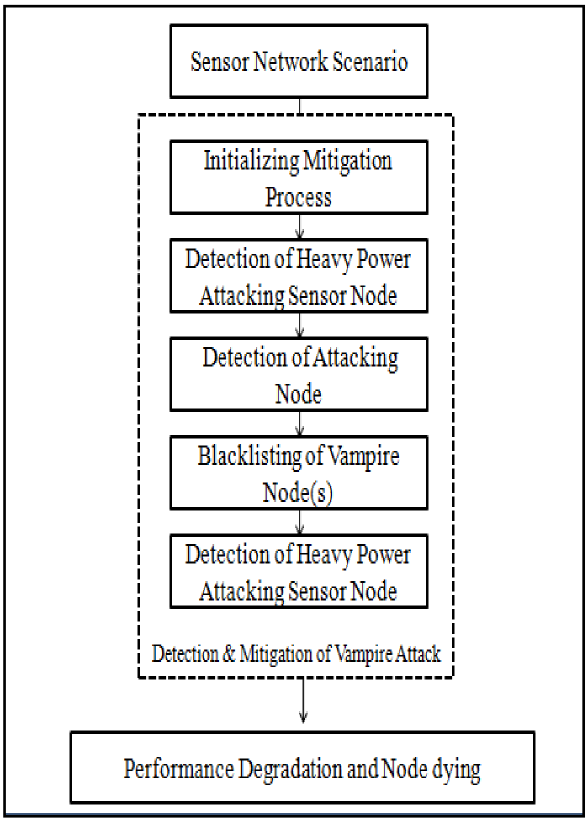
Sensor Network Scenario
Initializing Mitigation Process
Detection of Heavy Power Attacking Sensor Node
Detection of Attacking Node
Blacklisting of Vampire Node(s)
Detection of Heavy Power Attacking Sensor Node
Detection & Mitigation of Vampire Attack
Performance Degradation and Node dying

Figure 3.b: Mitigation of Vampire Attack

4. IMPLEMENTATION & RESULT ANALYSIS

The main requirement for the proposed work is to first observe the actual performance of network by applying security threats to it and analyze the activities of a network under different environments. On the basis of the outcome and observation the desired algorithm would be designed which will be tested in the same environment in order to perform comparison analysis and observe that the algorithm gives required results.

The routing algorithm utilized in the Wireless Sensor Network is vulnerable to the various types of attacks mentioned earlier such as denial of service attack, warm-hole attack, black hole attack and heavy traffic attack. In order to resolve this issue, firstly an impact analysis study has to be performed on the network which will provide the vulnerability level i.e. up to what extent the network is vulnerable to the above mentioned threats. This study will provide a base for designing the algorithm and its requirements. This work will completely analyze the basic security threats on the mobile ad hoc Networks. The objective of this study is to minimize the security threats in the WSN in order to transmit data without any problem.

The proposed work will perform a security aware formulation and also define it in order to enhance the security in WSN. In order to simulate our research NS2.35 will be used. Network Simulator (NS) is a simulation tool developed and maintained by researchers at Berkeley. It is discrete event and object oriented simulator developed for networking research. It provides substantial support for simulation of TCP, routing, and multicast protocols over both wired and wireless networks. NS-2 is written in C++ and Object Tool Command Language (OTCL). User uses the scripting language OTcl for defining the network and other feature like traffic or routing protocols, agents etc. The OTcl script written by user is used by ns during the simulations. The result of the simulations is provided in an output trace file. NS2 also provide an animation tool called Network Animator (NAM) to visualize the packet traces.

Highlights of implementation of proposed solution are following as :

- Creation and Performance Analysis of Normal WSN for variable number sensor nodes.
- Creation and Deployment of Vampire attack in sensor networks
- Detection of malicious node using energy consumption analysis.
- Identify most used sender address and create list of suspected nodes.
- Blacklist suspected nodes to prevent network from unwanted flood and overwhelming communication.

The complete work will not only avoid vampire attack but also avoid the situation of power drain. Proposed work will help to sustain node life as it naturally deserve.

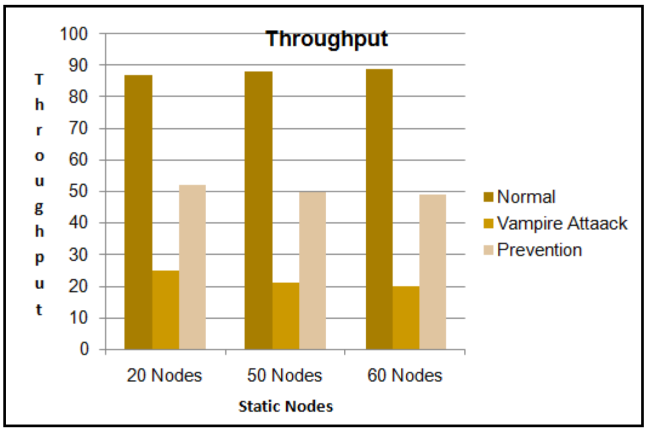

Figure 4.a: Throughput for Static Nodes

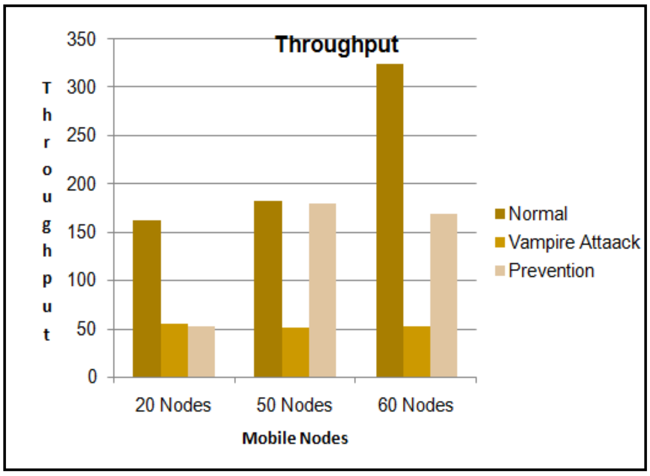

Figure 4.b: Throughput for Mobile Nodes

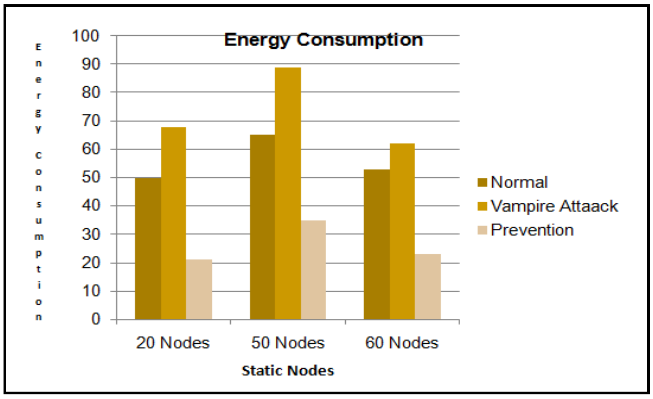

Figure 4.c: Energy Consumption for Static Nodes

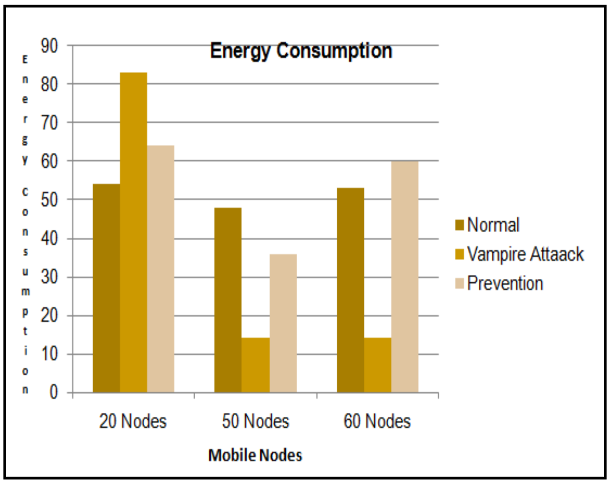

Figure 4.d: Energy Consumption for Mobile Nodes

5. CONCLUSION

The complete study is based on Vampire Attack which is a resource depletion attack in Wireless sensor network. In the analysis phase of study, it is observed that battery power is the most important resource for Wireless Sensor Network, but due to its broadcasting behavior and dependencies on traditional mobile ad-hoc routing protocols it is very easy to target the battery of a sensor node and it is possible to drain it with the help of compromised nodes which are named as Vampire Node.

In first phase, Vampire attack is deployed in AODV by configuring a new protocol named VampireAODV, to analyze how it affects the availability of sensor nodes. After that, by observing the difference in the battery consumption by victim nodes in normal case and under the effect of Vampire Attack, the mitigation approach is integrated in AODV routing protocol. After implementing the proposed solution, certain parameters are observed for the performance analysis under attack and under mitigation. The complete implementation work ends with certain observations which are listed below;

1. High impact on throughout has been observed in mobile state in comparison with stationary state.
2. Proposed solution performs better with high number of nodes in comparison to low number of nodes.
3. Heavy impact of vampire attack on battery model has been recognized for static and mobile positions.

The complete observations from the result acquired, shows that the approach is successfully capable of mitigating the effect of up to two Vampire nodes in a Wireless sensor network. An improvement in the remaining battery of victim nodes can be seen from the results

6. REFERENCES

[1] Sen, J., “A survey on wireless sensor network security,” published in “International Journal of Communication Networks and Information Security (IJCNIS)”, Vol 1, No 2, August 2009, pp. 55-78.

[2] Sangwan,A., Sindhu,D., Singh, K., “A Review of various security protocols in Wireless Sensor Network”, IJCTA, ISSN:2229-6093, vol. 2 (4), july-august-2011, pp.790-797.

[3] Gowrishankar.S , Basavaraju, T.G., Manjaiah D.H, Sarkar, S., “Issues in Wireless sensor networks” In Proceedings of the World Congress on Engineering vol I, 2008.

[4] Pathan,A.S.K., Lee, H.W., Hong, C.S. “Security in Wireless Sensor Networks: Issues and Challenges ” ICACT ISBN 89-5519-129-4, pp 1043-1048, 2006.

[5] Balakrishna, R., Rajeshwar Rao, U., Geetahanjali, N., “Performance issues on AODV And AOMDV for MANETs”, published in “International journal of Computer Science and Information (IJCSIT),” vol. 1 (2), 2010, pp. 38-43.

[6] C.E. Perkins and E.M. Royer, “The Ad Hoc On-demand Distance Vector Protocol”, 2000 pp. 173-219.

[7] Panday, M., Shriwastava, A., “A Review on security Issues of AODV routing protocol for MANETs”, IOSR Journal of Computer Engineering(IOSR-JCE), e-ISSN:2278-0661, p-ISSN:2278-8727 vol. 14, Issue 5 (Sep. - Oct. 2013), pp.127-134.

[8] C.E. Perkins and E.M. Royer, “The Ad Hoc On-demand Distance Vector Protocol”, 2000 pp. 173-219.

[9] Y. Hu and A. Perrig, "A Survey Of Secure Wireless Ad Hoc Routing", published in IEEE Security & Privacy, 2004. pp. 28-39,

[10] Eugene Y. Vasserman, Nicholas Hopper, "Vampire attacks: draining life from wireless ad-hocsensor networks", IEEE Trans on mobile computingvol, vol. 12, no. 2, 2013.

[11] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, Scott F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols", IEEE Transactions on Vehicular Technology, vol. 58, no. 1, 2009.