Prevention of Vampire Attacks in Wireless Sensor Network

Damayanti D. Pawar
Post Graduate Student
Department of Computer Engineering,
C.I.I.T, Indore

Megha Singh
Assistant Professor
Department of Computer Engineering,
C.I.I.T., Indore

ABSTRACT

In today's world of research computing wireless sensor networks are the widely used for various operations. These networks contain number of sensor nodes whose task is to collect data and send it to the data aggregator for further processing. For these type of networks low powered and energy efficient devices are mostly required for the collection of data because of which energy management becomes an important part of them. One of the major problems related to security which is faced by these networks is that of vampire attacks. These attacks are launched by the adversaries in order to drain the energy from the network so as to create denial of services and abruption. This paper focuses on the effects of vampire attacks on wires less sensor networks especially on Dynamic State Routing Protocol (DSP) & Destination-Sequenced Distance-Vector Routing (DSDV) protocols. The methods are also given to prevent the network from these attacks. The results are collected by performing the attacks on actual networking scenario & applying our system to prevent the attacks.

Keywords

Vampire Attacks, Denial of Service, Wireless adhoc networks

1. INTRODUCTION

Wireless Sensor Networks are becoming more essential for day today used technology in various fields like educational, agricultural, commercial, military applications and people. Because of their ad-hoc nature they are more vulnerable to denial of service attacks. The network is also known as ad-hoc network because it does not rely on any pre existing structure. The life of these ad-hoc networks depends upon the node's battery power. If the battery power decreases then the data loss may occur or even the network may collapsed due to this. While studying it is observed that two Vampire attacks namely "carasoul attack" [2] and "stretch attack" [2] are mostly affecting the protocols involved in ad-hoc networks to drain the battery power of networks. These attacks directly decrease the battery power of nodes in order to collapse the network. Vampire attacks are not protocol-specific and they do not depend on design properties or implementation faults of specific routing protocols, but rather exploit properties of protocol classes such as link state ,distance-vector, source routing, and geographic and beacon routing. Vampire attacks do not depend on flooding the network with large amounts of data rather try to transmit as little data as possible to get the largest energy drain which prevents a rate limiting solution. These attacks are very hard to detect and prevent because Vampires use protocol compliant messages. If a system is designed to overcome the effects of Vampire attacks on the said protocols then it will automatically reduce the overloads in ad-hoc networks which in turn will help to increase the battery life of network. So the paper gives description about the two Vampire Attacks, their effects on the protocols and a system to prevent the protocols from these attacks.

2. LITERATURE SURVEY

A great deal of research has been done in this area [3][4][5] which gives brief details about denial of service attacks and their effects on ad-hoc networks. Eugene. Y. Vasserman and Nicholas Hopper[1] explores resource depletion attacks which are also known as "Vampire Attacks" [2] at the routing protocol layer, which permanently disable networks by quickly draining nodes battery power. They have given detailed information of various vampire attacks and their effects on the ad-hoc networks. Also they have stated various methods to prevent the network from these attacks. This paper mainly focuses on effects of vampire attacks on Dynamic State Routing Protocol and Destination Sequenced Distance Vector Routing Protocol. A brief introduction of these two protocols and the effects of vampire attacks on these protocols is given in our earlier work [2]. Some new research work in this field includes various implementations and theoretical work like [6] illustrates a technique to tolerate the attack by employing the Cluster Head. In case of each Vampire attack, the Cluster Head employs in this situation and distributes the packet to destination without dropping the packet. Thus gives a successful and reliable message delivery even in case of Vampire attack. In [7] the authors discussed about the method to reduce the vampire attack using PLGP-a identifying malicious attack. Next paper [8] explores the energy issues and attacks that challenge that are faced by Ad-Hoc WSNs and eventually the future IoT. It also discusses a resilient strategic approach for handling energy attacks. All the above work done in this area is focused on various protocols and the effects of vampire attacks on them. The proposed system will try to achieve the finest solution in all of them and also it will be performed on actual network scenario instead of network simulator.

3. PROPOSED SYSTEM

This section briefs about the working of proposed system.

Carousal attack :The steps of working are as follows:

1. Start the nodes involved in data transfer.
2. Send the message from sender which will travel from predefined route.
3. Because of carasoul attack, the nodes will go in infinite loop and packets will never deliver to the receiver.
4. Then run the system in prevention mode.
5. Now the prevention mode will prevent the attack and the packets will deliver to the receiver.

Stretch attack: The steps of working are as follows:

1. Start the nodes involved in data transfer.
2. Send the message from sender which will travel from predefined route.
3. When stretch attack will perform, purposely long routes will be selected in order to delay the delivery of packets.
4. Then run the system in prevention mode.
5. Now the prevention code will prevent the attack and the packets will deliver to the receiver without delay.

4. IMPLEMENTATION

The system is simulated using Java. Two algorithms are used for Carasoul Attack and Stretch Attack. In this simulation scenario a wireless network is implemented. After the network preparation a malicious node is deployed on the network this simulation is used to demonstrate the effect of vampire attack thus after simulation the performance of network is estimated. Then Simulation of the proposed secure routing strategy under Attack is shown in which the proposed secure mechanism for vampire attack detection and prevention is demonstrated. In order to prepare the simulation the wireless sensor network is implemented with the modified AODV routing protocol for preventing the effects of the Vampire attack.

For analysing the performance the following parameters used are energy consumption, delay and packet delivery ratio which is a major factor and is given as

$$packet\ delivery\ ratio = \frac{total\ delivered\ packets}{total\ sent\ packets}$$

5. RESULTS AND DISCUSSIONS

This section describes the results obtained from the implemented system.

The system was implemented on real ad-hoc network using two protocols by performing carasoul & stretch attacks on the network. It shows the effects of vampire attacks on the protocols and prevention mechanism for the same. The three parameters namely Time Delay, Energy and Packet Delivery Ratio were recorded when the system is in attack and in prevention mode of system to check the usability of the system. The summarised results are tabulated in table 1. It can be seen that the proposed system gives better results by preventing the ad-hoc network from attacks. Also the energy required to nodes for delivery of packets is less in prevention mode as compared to attack mode.

Table 1: Results and Comparisons

Sr. No.	Attack	Time Delay	Energy	Packet Delivery Ratio
1	Carasoul	8750	2048	1024
2	Normal	6584	1568	1456
3	Stretch	9865	3056	985
4	Normal	3568	1589	1352

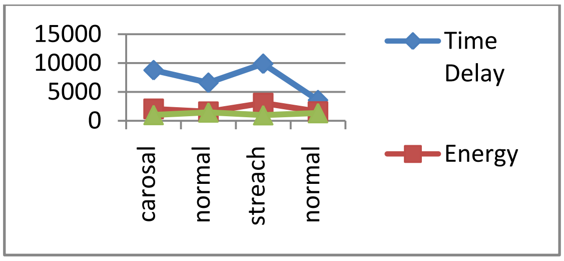

Fig: Graph showing difference in attackmode and prevention mode

6. CONCLUSION

We defined Vampire attacks, the battery depletion attacks that use routing protocols to permanently exhaust ad-hoc wireless sensor networks by consuming nodes battery power. Firstly we discussed the use of ad-hoc wireless networks in today's world. Then we have discussed about the vampire attacks and their effects on Wireless Sensor networks using two protocols i.e. DSR & DSDV. Then the system was described in detail and finally we discussed results recorded by performing the Carasoul attack and Stretch attack in actual network environment and using the system to prevent network from these attacks. The result shows that the energy required to deliver packets is less by using the implemented system. In future we plan to use the implemented system on networks with more nodes. Also it will be useful for mobile networks.

7. REFERENCES

[1] Eugene Y. Vasserman, Nicholas Hopper- Vampire attacks: Draining life from wireless Ad-hoc Sensor networks IEEE TRANSACTIONS ON MOBILE COMPUTING VOL.12 NO.2 YEAR 2014

[2] Damayanti D. Pawar and Megha Singh, Dealing with Vampire Attacks: A Survey. . International Journal of Scientific Research and Publications92(16):23-29, April 2014. Published by Foundation of Computer Science, New York, USA.

[3] Yih-Chun Hu, David B. Johnson, and Adrian Perrig, SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks, IEEE workshop on mobile computing systems and applications, 2002.

[4] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, Effects of denial-of-sleep attacks on wireless sensor network MAC protocols, 58 (2009), no. 1.

[5] Charles E. Perkins and Pravin Bhagwat, Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers, Conference on communications architectures, protocols and applications, 1994

[6] Gowthami. M, Jessy Nirmal.A.G, P.S.K.Patra, Mitigating Vampire Attack in Wireless Ad-Hoc Sensor Networks

[7] Trupti A Borgamwar , Kanchan Dhote , Review of Resist to Vampire Attack using Wireless Ad-hoc Sensor Network

[8] Tawseef Ahmad Naqishbandi ,Imthyaz Sheriff C, A Resilient Strategy against Energy Attacks in Ad-Hoc WSN and Future IoT