ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Vampire Attacks on Wireless Ad Hoc Sensor Networks

Tushar Thosar[1], Anuradha Joshi[2]

P.G. Student, Department of EXTC Engineering, VIT College of Engineering, Wadala, Maharashtra, India[1]

Associate Professor, Department of EXTC Engineering, VIT College of Engineering, Wadala, Maharashtra, India [2]

ABSTRACT: Wireless sensor networks become popular at the start of this millennium due to presence of small-sized sensors with low power deployed for monitoring large area. There is large amount of research being done to increase life of these networks, where lifetime of network is measured from time of deployment to the time when one of the nodes becomes in-operational as power supply is completely used up by the node. It is commonly known as first node failure.In this paper we have discussed the effect of attacks on routing protocols which are designed to be secured. These attacks are known as Vampire attacks and they can permanently disable the network by using all the battery power of different nodes. Vampire attacks are not designed for any specific protocols and are devastating, difficult to detect and can be easily carry out using a few one malicious insider sending only protocol compliant messages. We proposed a EWMA method to control the damage caused by these vampire types of attacks during the pocket forwarding phase.

KEYWORDS: Vampire attack, Wireless Sensor Network, EWMA.

I. INTRODUCTION

Wireless communication has become so popular and important in last few years that we cannot imagine a world without them. Apart from the conventional techniques like mobile phones and WLAN, there are new techniques for wireless communication coming into picture which are ad hoc and sensor networks. Ad hoc and sensor networks consist of different nodes which communicate with each other through radio but do not require any additional support. A network of small embedded devices known as sensors communicating wirelessly is known as a wireless sensor network. These sensors are placed strategically inside a physical medium so that they can measure physical parameters from the surrounding and give this information to the system. The nodes use broadcast communication and network topology keep changing constantly because the nodes are prone to fail. There for node should be autonomous and they will be disregarded. These devices have limited power, limited memory and low computational capabilities. The main issues with WSNs that should be studied are scalability feature, limited energy to supply the device and their connection strategy for communication.

II. RELATED WORK

Resources in the wireless network sensors are limited and due to this there are several challenges in front of researchers and developers in this area. The algorithms written for these networks are framed with parameters like bandwidth, computational complexity and memory due to the hardware constraints. The cost of these networks can be very high as power consumption becomes higher. So energy efficient wireless sensor networks are priority to most developers.
The power exhaustion attack also called as “sleep deprivation attack” in many cases as this attack prevents nodes from getting into the sleep cycle and drains their batteries quickly. Latest research in this field is only checks attack at MAC layer. There are brief mentions of malicious cycles but there is no effective discussion other than increasing efficiency of underlying MAC layer and routing protocols or switching away from source routing.

There are several studies in denial of service attack on hardware network. These mention adversaries who prevent route setup, disrupt communication or sometimes make routes through themselves to drop, manipulate or monitor packets.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

The security of the networks can be affected by denial of service attack. The path discovery success based security approach of many networks cannot protect against vampire attacks. This is because vampire attacks do not use or return illegal paths or prevent communication in the short term.
There are also work going in minimal energy routing aims at increasing life of power constrained networks by using minimum energy in sending and receiving packets. But vampire attack can increase energy in such networks also. Vampires can create packets which will travel more nodes than required, so there is more expenditure of energy even if the nodes spend minimum amount of energy to transmit packets. Thus it is very expensive to send packets in the presence of vampires.

III. COMPARISON OF DIFFERENT TYPES OF ATTACKS:

1. Sleep Deprivation Torture attack:
   - It is most dangerous attack and it causes minimization of sensor node's lifetime by maximizing their power consumption
   - Attacks innocent nature makes it difficult to detect it
   - It is difficult to prevent sensed data with traditional security system as we have limited resources
   - To detect these attacks security mechanism must be equipped with efficient resource utilization, especially power
   - It only detects attacks at Medium Access Control(MAC)
2. Resource exhaustion attack:
   - These attacks occur when resources are not available for service
   - So the nodes deny the service as they don't have the required resources for thatparticular service
   - It thus stops nodes performing current actions
   - Resource unavailability is mentioned at MAC and transport layer
   - It offers rate limiting and elimination of insider adversaries.
3. Flood Attack:
   - It is a type of denial of service attack which occurs when network is flooded with large no. of traffic
   - It results in incomplete connection request as network can no longer perform connection requests
   - Incomplete connections at the server or host is result of connection flooding due to which memory buffer of server gets filled
   - Thus the connections are not made as this memory buffer is full and hence the denial of service
   - The nodes which produce burst of traffic are punished but less data is sent.
4. Reduction of Quality (RoQ) attack:
   - These are new breed of attacks which break adaptive mechanism in todays network and computing systems.
   - Because of these attacks adaptive mechanism is always oscillated between overload and under-load conditions.
   - It can cause long term degradation in network.
   - It focus is always on transport layer and ignores routing protocols.
5. DoS Attacks:
   - The purpose of this attack is to make resources unavailable to the user network so that it cannot perform the specified action or service.
   - The main motive of these attack is to interrupt or suspend the services of the host connected to network, temporarily or permanently
   - These attacks can occur only to traditional DoS and doesn't work on intelligent adversaries.
6. Wormhole attack:
   - It is severe attack on ad hoc network
   - It can occur even if no host is compromised and there is total authenticity and confidentiality in all communication

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

- In these attacks, attacker records message at one node of network then tunnel them at different location in the network and then retransmits them from there into the network.
- It is a serious threat to wireless networks like ad hoc network routing protocols and location-based wireless security systems.

7. Directional Antenna attack:
   - Directional antennas are increasingly being used for increasing capacity and connectivity of ad hoc networks.
   - Directional transmission increases energy efficiency
   - Due to large range of directional antennas there is reduction in hops routing but it can also get connected to unwanted malicious nodes. Thus disrupting rout discovery. Various protocols were used for security of wireless sensor networks.
   -

The comparison of protocols is as follows:

Sr. No.	SNEP Protocol	REWARD	Statistical En-Route Filtering
1.	It is basic component of SPINS designed for secure key distribution	It is proposed to protect against black hole attack and malicious nodes	It is technique to prevent attack on compromised sensor nodes as they can insert wrong report in network and can cause depletion of resources at the nodes and false alarm.
2.	It defines primitives for authentication of sensor node, data confidentiality and data integrity	It works on geographic routing which uses two kinds of messages MISS and SAMBA	This technique can detect and destroy false reports in network using authentication cades which are MAC
3.	SNEP is used cipher plain text with CTR encryption algorithm	MISS gives identity of malicious sensor node while SAMBA is used to recognized the detected black hole attacks	This technique works on collective information generated by neighbouring nodes whenever an event occurs
4.	It has lower data freshness	It uses broadcast inter radio behaviour to detect black hole attacks	This information is a legitimate report which is forwarded and verified by each node and it is dropped if found incorrect at any step
5.	In this protocol every message has message authentication code (MAC) which is computed using cipher data with CBC-MAC algorithm	It is possible because when node becomes out of control it maintains distributed database and store it for future use	In case the false report reaches the sink node then it is sink node who is responsible to check its correctness
6.	At the receiver end it is recomputed and matched with the sender's MAC	Its only drawback is more energy consumption	Its drawback is that it causes delays and increases communication overhead and energy consumption

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

IV. ENERGY DRAINING ATTACKS (VAMPIRE ATTACKS)

When a message created and sent by node leads to more energy consumption by network and thus causes a slow depletion of node's power source it is known as Vampire attack. The node becomes malicious as it is creating these attacks on the network.

1. Attack on Stateless Protocols
   In this system the source node provides entire path in the packet header. The intermediate nodes do not make any decision about the route and follow the route given by source node in packet header. Thus source node has to make sure that path is correct and each node is neighbour of the previous hop. This requires very little forward logic at intermediate nodes and entire route can be made sender authenticated by digital signature.
2. Attack on Stateful Protocols
   In this method network nodes are aware of the network topology and its state and make local forwarding decision based on stored data. There are two types of this method 1) link-state 2) distance-vector. In link-state every node keep record of up or down state of links in the network and these records are updated every time when a link goes down or new link joins the network. Distance-vector method gets track of next hop to every destination.

There are mainly two types of vampire attacks:-

1. Carousel Attacks
2. Stretch Attacks

Sr. No.	Carousel Attacks	Stretch attacks
1.	In this attack packets are sent with a route composed of loop so the same node appears again and again	This attack creates artificially longer route so that packet has to travel more than the optimal path
2.	This increases the routing length but number of allowed entries in source node can limit it.	Thus more nodes are used for transferring packets leading to more energy usage causing battery drainage and it is not honest scenario as path is artificially created
3.	Attack has theoretical limit which is energy usage increase factor of $0(\lambda)$ where λ is maximum route length	Here energy usage increase factor is $O(\min(N,\lambda))$, where N is number of nodes in the network and λ is maximum path length
4.	It increases overall energy consumption by factor of 3.96 per message	It increases energy usage by factor of 10.5 per message

Though Stretched attack is less damaging than Carousel attack as number of hops per packet depends on number of network nodes, there is chance of a combined attack so that packet can be kept in the network for longer route. This results in more energy consumption as stretched cycle is always in the loop. Thus route loops should be detected and removed to protect the network from combined attack.

V. CONCLUSION

In this paper we have seen Vampire attacks which are a new class of attacks. These attacks use routing protocols to permanently disable ad hoc wireless sensor network by draining battery power of nodes. These attacks are not dependent on particular protocols or implementation but shows vulnerabilities in different protocol classes.

REFERENCES

[1] Eugene Y. Vasserman and Nicholas Hopper "Vampire Attacks: Draining Life fromWireless Ad Hoc Sensor Networks"- IEEE TRANSACTIONS ON MOBILE COMPUTING,VOL. 12, NO. 2, FEBRUARY 2013.

[2] Frank Stajano and Ross Anderson, The resurrecting duckling: securityissues for ad-hoc wireless networks, International workshop on Security protocols, IEEE 1999.

[3] Haowen Chan and Adrian Perrig, Security and privacy in sensor networks, Computer 36 , IEEE 2003

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

[4] Denial of service attacks(Timothy J. McNevin, Jung-Min Park), IEEE 2004
[5] Path-quality monitoring in the presence of adversaries(Sharon Goldberg, David Xiao),IEEE 2008.
[6] Packet leashes: A defence against wormhole attacks in wirelessad hoc networks, INFOCOM, IEEE 2003.
[7] Securing ad hoc routing protocols,(Manel Guerrero Zapata and N. Asokan), IEEE 2002
[8] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc. Networks, "IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, IEEE Nov. 2006.
[9] J. Deng, R. Han, and S. Mishra,"Defending against Path-Based DoS Attacks in Wireless Sensor Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, IEEE 2005.