Vampire Attack: A Novel Method for Detecting Vampire Attacks in Wireless Ad –hoc Sensor Networks

Kalyani S Kumar
Department of ISE, GSSSIETW, Mysuru, Karnataka

Abstract: **Ad-hoc wireless networks are dynamic in nature. Ad-hoc networks are not depends on any predefined infrastructure. Whenever there is need of communication at that point these network can be deployed. In this paper we discuss Vampire attacks. All protocols susceptible for vampire attack. Vampire attacks are very easy to carry out throughout the network and difficult to detect. Wireless sensor networks (WSNs) are the foremost promising research direction in sensing and pervasive computing. Previous security work has focused totally on denial of service at the routing or medium access management levels. Earlier, the resource depletion attacks are thought about solely as a routing drawback, very recently these are classified into new category as "vampire attacks". Planned work examines the resource depletion attacks at the routing protocol layer that disable networks permanently by quickly debilitating node's battery power.**

I. INTRODUCTION

A wireless sensor network contains number of sensors that are distributed across a wide geographical area. Several applications uses a constitute network which is formed by autonomous sensor [1]. The applications are structural health monitoring, health-care monitoring, industrial monitoring, instantly deployable communication for military, on-demand computing, inventory tracking, power management, factory performance, power, smart sensing thereby information or data gathering and processing, seismic detection and acoustic detection[2].The life of network plays a crucial role in such applications. Many researches focus on increasing the lifespan of WSN [3]. One new type of resource (energy) depletion attack is known as vampire attack [5] which exhausts the battery power of the node to disable the whole network. An adversary compromised the vampire node in sensor network. This node continuously sends messages to other nodes so each node in the network loses energy faster causing the failure of the whole network soon. The vampire attack can target any routing protocol and does not specific to particular protocol. They are difficult to detect because they do not alter the original message. There are two types of vampire attacks stated in [5] Carousel attack and Stretch attack. In carousel attack a series of loop is formed between the source and the sink node. So the route length is increased and goes beyond the limit of nodes in the network. Due to this energy consumption of nodes increases and thus minimizes the network lifetime. In stretch attack, artificially long route from source to sink is made by an adversary causing packets to traverse a larger route and draining extra energy.

II. RELATED WORK

In 2013 Eugene Y. Vasserman and Nicholas Hopper [5] introduced a definition for vampire attacks. The authors introduced PLGPa protocol which tries to overcome the damage from Vampire attacks. But during the topology discovery phase satisfactory solution for Vampire attacks is not offered and further modifications to PLGPa are suggested. In 2014 Sunil Bhutada, Kranthi Kumar.K, Manisha.K [6] proposed a system which mitigates the vampire attacks by saving bandwidth, power and time. At each node to detect the presence of vampire attacks, route validation will be checked and if present avoids it immediately. Clean-Slate Sensor Network Routing is used to forward the data packets safely. In 2014 Mrs. R.Abirami, and Mrs.G. Premalatha [7] proposed some defenses against vampire attacks and described Interior Gateway Routing Protocol (IGRP) protocol which is a Cisco-proprietary Distance-Vector protocol. This protocol provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destination. Also in 2014 Divya and Vanitha [8] introduced a valuable secure protocol to prevent attacks in wireless ad hoc sensor networks. The network configuration, key management and communication phase are the three phases of VSP. Elliptic Curve Cryptography (ECC) approach is used with VSP. E. Mariyappan and Mr. C. Balakrishnan [9] proposed A Sensor Network Encryption Protocol using boundary recognition technique, recursive grouping algorithm and jump point algorithm so that the correct path is produced to prevent the vampire attacks in forwarding phase. Damodhar and Umakant [10] described the Energy Weighted Monitoring Algorithm to overcome from resource consumption attack. For consuming the nodes energy, two phases are initialized in EWMA. According to simulation results the proposed technique performs well. Sivakumar and Murugapriya [11] described Optimal Energy Boost-up protocol for providing the security. It was found that the energy of network based on the location is increased in forwarding phase. In 2014 Soram rakesh singh and Narendra [12] presented MDSDV protocol. M-DSDV protocol is designed to combat the routing loop problems. It was observed that, this system has reduced the damage from vampire attacks in forwarding phase. José Anand and Sivachandar [13] presented the vampire attacks detection in wireless sensor networks. The effect of vampire attacks on AODV is proposed for providing the security. During the forwarding phase, energy of the network is increased. In 2015 Lina R. Deshmukh, and A. D. Potgantwar [14], proposed No-Backtracking property scheme to achieve high efficiency and secure authentication. Within the network by using group identification method the nearest neighbour node is identified. The PLGP protocol is a slate secure routing protocol, which is used to prevent vampire attack during packet forwarding.

III. ATTACKS ON STATELESS PROTOCOL

In these protocols, nodes are not aware of states of network. Source node defines the route on which packet must be travelled, so sender must ensure that the path which is defined must be exist. An intermediate node does not make any decision about packet forwarding. When sender sends packet at defined route, at that time, path is stored in packet header for some period which can be useful for another time. That's why intermediate nodes needs very little forwarding logic [2]. Carousel attack: An adversary sends a packet with a route composed as a series of loops, such that the same node appears in route many times. Stretch attack: A malicious node construct artificially long source routes, causing packets to traverse a larger than optimal number of nodes. 1.2 Attacks on stateful protocols In Stateful protocols each node knows the topology of network and aware of state of every other node in the network. Intermediate nodes make independent decision based on stored state. Following are some attacks: Directional antenna attack: Vampires have less control over packet when packet is forwarded independently, but malicious node may forward packet at any part of network that is called directional antenna attack. Malicious discovery attack: Sender node send discovery packet, malicious nodes also send discovery packet in network. The nodes who listens discovery message they send reply to the sender nodes but as some discovery messages are malicious, so reply to those messages may not reach at its destination due to malicious nodes not found. This leads traffic in network with loss of energy.

IV. MITIGATION METHOD

Carousel attack sends packet in loop. We can avoid this by using some extra forwarding logic and it will leads more overhead. In DSR, loop can be detected, but it will not check path in forwarded packets. In source routing protocol, path is signed by source. When loop is detected, it should be corrected and then sent on. Instead of correcting and sending again, dropping that packet is more convenient and beneficial. Stretch attack is more difficult to prevent. If intermediate nodes not takes independent decisions and uses strict source routing that is packet must travel only the path which is defined by source. And if that path is not present or damaged International Journal of Computer Applications (0975 – 8887) problem is created. In loose source routing if header has defined path, but if intermediate node knows another better route then intermediate nodes may change the route. Now, In this case malicious nodes may send packet through longest route or on route which is not exist. Here is a advantage that intermediate nodes uses cached route, which are already discovered and stored.

V. CLEAN SLATE ROUTING

This protocol is used to resist vampire attack during forwarding phase. Also known as PLGP, as invented by Parno, Luk, Gaustad and Perrig . This is original version which is discovered for security purpose but this protocol also susceptible for vampire attack. There are two phases in this protocol first is topology discovery phase another is packet forwarding phase. Topology discovery phase: Discovery phase• organizes nodes into tree for addressing purpose. Nodes announce their existence in network by broadcasting their certificate of id and its public key. By grouping process tree is formed. Each node starts grouping with its group size 1 and virtual address 0. Then neighboring nodes overhears and form a group with that node and address becomes 0 and 1 for each node. This process will continue until all nodes forms in a single tree. There are another groups are there which are away from another group and so they are out of radio range and they can't communicate each other. These two long distance groups communicate through gateway nodes. Packet forwarding phase: Once nodes are arranged in tree like structure then it is easy for packet to traverse a path using address defined. Sender sends hello message to near nodes they overhear and send reply. Sender sends data packets to neighboring nodes after receiving reply. Each node makes independent decision by using most significant bit of address field.

Provable security against vampire attack To avoid vampire attacks there is need to keep track on the path travelled by packet so we can avoid to forward it at any part of network. First we define a no-backtracking property, when packet travelled same number of hops with and without presence of malicious nodes and packet makes continuous progress towards its destination at that time that packet satisfy no-backtracking property. In Clean Slate routing protocol, paths are bounded by tree. In other protocols tree is not used for addressing purpose. So Clean Slate routing protocol is different from other protocols. Every node have same copy of tree for addressing. Every node can verify the optimal next logical hop. This is not enough for no-backtracking property because adversaries can always lie.

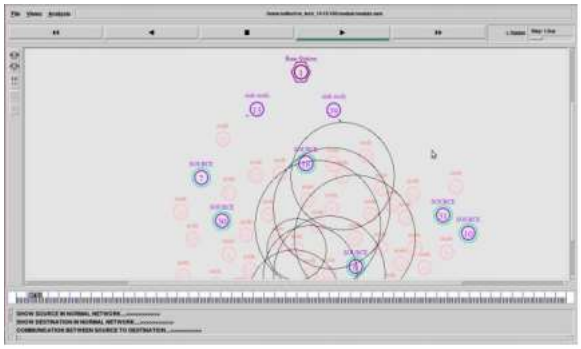
No-backtracking implies vampire resistance No-backtracking property resists vampire attack in packet forwarding phase. The reason of success of stretch attack is the intermediate nodes do not check whether packet choses optimal path or does it makes continuous progress towards destination? Adversaries send packet at any part of network. Clever adversaries can affect any type of routing protocol, so we can check packet progress at each node, if packet makes continuous progress towards destination.

VI. PROPOSED METHODOLOGY

From the review of security techniques, it is observed that most of the security techniques provide solution in packet forwarding phase only. Proposed Enhanced PLGPa is planned to be at the deficiencies of PLGPa. The proposed work mainly focused on avoiding vampire attacks in the discovery phase of PLGP. A malicious node (vampire) would send high energy signal and usage the packet flooding and RREQ flooding to establish the malicious connection. For trusted nodes estimation signal strength of the group joining messages is checked for each node. In order to provide solution during discovery phase the threshold concept is utilized. This threshold value is used to determine the suspicious node. Now the broadcast values of nodes are compared to the estimated threshold value. The nodes will be divided into two groups such as suspicious node or normal node. ALGORITHM 1. Start 2. Nodes broadcast the group joining request. 3. Signal Strength of each node will be calculated. 4. Mean threshold value will be calculated. 5. Attackers are started through network 6. PLGPa process started 7. If (signal strength of node < Mean Threshold) 8. Allow the connection to neighboring node. 9. Else 10. Mark node as vampire node and removed from network. 11. Start communication between source and destination. 12. End if 13. End

VII. SIMULATION AND RESULTS

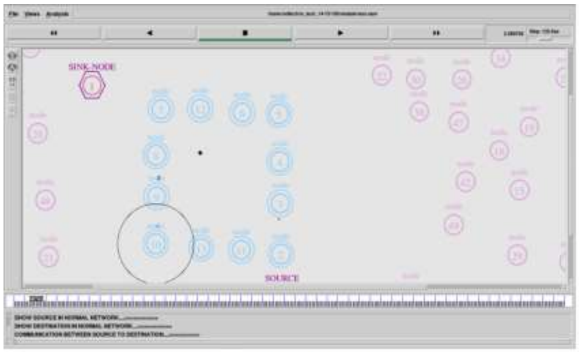
Simulation is done on NS 2.35. Sensor network with 50 nodes is created. Normal communication between nodes, sink nodes and base station takes place. Figure 1 shows network set up and communication.



SHOW SOURCE IN NORMAL NETWORK.....
SHOW DESTINATION IN NORMAL NETWORK.....
COMMUNICATION BETWEEN SOURCE TO DESTINATION.....

Fig 1: Wireless Sensor Networks and Communication between nodes.

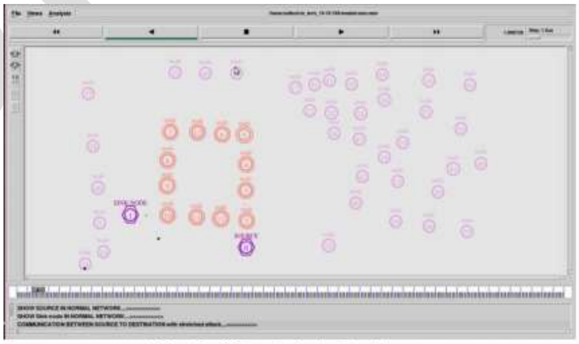
The carousel attack is carried on wireless sensor networks shown in figure 2. In this type of attack a series of loop is formed between the source and the sink node. So the route length is increased and goes beyond the limit of nodes in the network. Due to this energy consumption of nodes increases and thus minimizes the network lifetime. By a factor of O(λ) energy usage increases, where the maximum route length is λ. Energy consumption during attack is measured.



SHOW SOURCE IN NORMAL NETWORK.....
SHOW DESTINATION IN NORMAL NETWORK.....
COMMUNICATION BETWEEN SOURCE TO DESTINATION.....

Fig 2: Carousel Attack.

The stretch attack is carried on wireless sensor networks shown in figure 3. In this type of attack artificially a long route from source to sink is made by an adversary causing packets to traverse a larger route and draining extra energy. This attack causes a node that doesn't lie on optimal path to process packets. By a factor of O(min(N, λ)), where the number of nodes in the network is N and the maximum path length is λ. Energy consumption during attack is measured.



SHOW SOURCE IN NORMAL NETWORK.....
SHOW Sink node IN NORMAL NETWORK.....
COMMUNICATION BETWEEN SOURCE TO DESTINATION with stretched attack.....

Fig 3: Stretch Attack.

VIII. CONCLUSION

Simulation is done on NS2.35 simulator. A network of 50 nodes is created. Effect of Vampire attack is on network is measured. Energy consumption during carousel attack and stretch attack is determined. Proposed system detects suspicious node which causes vampire attack in the network. Prevention of vampire attack and comparison proposed work with existing work is left for future work.

REFERENCES

[1]. Th. Arampatzis, J. Lygeros, S. Manesis "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks", Proceedings of the 13th Mediterranean Conference on Control and Automation Limassol, Cyprus, June 27-29, 2005.

[2]. Murtadha M. N. Aldeer, “A Summary Survey on Recent Applications of Wireless Sensor Networks”, 2013 IEEE Student Conference on Research and Development (SCOReD), 16 -17 December 2013, Putrajaya, Malaysia.

[3]. Long Zhaohua, Gao Mingjun, “Survey On Network Lifetime Research For Wireless Sensor Networks”, Proceedings of ICBNMT2009.

[4]. Jyoti Kumari, Prachi, “A Comprehensive Survey of Routing Protocols in Wireless Sensor Networks”, 2015 IEEE Conference.

[5]. Eugene Y. Vasserman, Nicholas Hopper, “Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks”, IEEE transactions on mobile computing, VOL. 12, NO. 2, February 2013.

[6]. Sunil Bhutada, Kranthi Kumar.K, Manisha.K, “A Novel Approach for Secure Routing Protocol: To Improve Life of Network”, 2014 IEEE Conference.

[7]. Mrs. R. Abirami, Mrs. G. Premalatha, “Depletion of Vampire Attacks in Medium Access Control Level using Interior Gateway Routing Protocol”, ICICES2014 - S. A. Engineering College, Chennai, Tamil Nadu, India.

[8]. K. Vanitha, V. Divya, “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 3, Special Issue 3, 2014.

[9]. E. Mariyappan, Mr. C. Balakrishnan, “Power Draining Prevention In Ad-Hoc Sensor Networks Using Sensor Network Encryption Protocol”, ICICES2014 - S. A. Engineering College, Chennai, Tamil Nadu, India.

[10]. B. Umakanth, J. Damodar , “Resource Consumption Attacks in Wireless Ad Hoc Sensor Networks” international Journal of Engineering Research Volume No.3 Issue No: Special 2, pp: 107-111, 2014.

[11]. K. Sivakumar, et.al, “Efficient Detection and Elimination of Vampire Attacks in Wireless Ad-Hoc Sensor Networks” International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, 2014.

[12]. Soram Rakesh Singh, Narendra Babu C. R, “Improving the performance of energy attack detection in wireless sensor network by secure forwarding mechanism” International Journal of Scientific and Research Publications, Volume 4, Issue 7, 2014.

[13]. Jose Anand, K. Sivachandar, “Vampire Attack Detection in Wireless Sensor Network” International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 4, 2014.

[14]. Lina R. Deshmukh, A. D. Potgantwar, “Ensuring an Early Recognition and Avoidance of the Vampire Attacks in WSN using Routing Loops”, 2015 IEEE International Advance Computing Conference (IACC).