International Journal of Science Engineering and Advance Technology

Vampire Attacks: Draining Life From Wireless Adhoc Sensor Networks

Pavani Potnuri[1], Bharath Kumar Gowru[2], Venkateswara Rao Nadakuditi[3]
[1] Assistant Professor, [2]Assistant Professor , [3]Assistant Professor in Dept of CSE,
Amrita Sai Institute of Science & Technology,paripala,Krishna dist.A.P
Email:pavani_875@yahoo.co.in, bharath.kumar436@gmail.com, n.venkat056@gmail.com

Abstract: ***Ad hoc less power wireless networks are one of the current topics in the field of security and pervasive computing. Most of the research work done before for improving the security of the networks in this area is mainly limited to the denial of message at the routing level or MAC levels. This project work investigates the attacks done with an aim of resource reduction at the routing protocol layer. These attacks can lead to the quick draining of the nodes battery power there by permanently disable the networks. These resource depletion attacks are called as "Vampire" attacks, which are not particular to any protocol, instead they depends on the general features of the routing protocols classes. In some of the bad cases, a particular vampire can increases network-wide bandwidth usage in the order of O (N). Present techniques to overcome these attacks were discussed, including one new protocol has been demonstrated which has successfully reduced the affects of the vampires while forwarding the packet as per the simulation results in the testing environment modeled in this work. A public key algorithm named Elliptic Curve Cryptography (ECC) algorithm is also used for more security provision.***

Keywords: sensor networks, security, protocol and Elliptic Curve Cryptography.

1.Introduction

Ad hoc wireless sensor networks (WSNs) is one of the areas where the research work has been pacing up dynamically from the past few years. WSN's[1] have so many applications already and are assuring many more new applications in coming future with the ongoing research works. The applications include supplying omnipresent computing power requirements in a on-demand scale, uninterrupted network connectivity, and provision of communication facilities for military and first responders in very instantaneous and rapid manner even under the conditions where there is no proper infrastructure is present at the times needed. Such networks observe factory performance, ecological surroundings, etc., to name some applications [2].

1.1 Background

With the growing applications and increased use of WSNs, they are becoming more and more vital in accomplishing everyday needs and tasks of people, organizations and society. Hence, the system i.e., WSNs for facilitating such type of requirements and needs should function in a very accurate manner without any faults or errors. Because, they can cause severe problems in proper functioning of the system, as they became part of the routine in performing tasks in our routine.

Lack of proper security and unavailability of WSNs will cause a major difference in general business operations as usual, other than that productivity loss, ecological disasters. Thus more availability of this type of networks is an important thing, and it should hold under malevolent conditions. Hence, any errors or faults in a WSN are not acceptable.

As we know, Ad hoc organization is very common and a general thing in a WSN. Because of this type of ad hoc organization, WSNs are more susceptible to DoS attacks. However, an amount of good research performed to protect WSNs against these DoS attacks, So that they can with stand and survive against them. Majority of solutions brought out by the researchers are able to prevent attacks when there is a low availability of the network, But due to lack power in addressing the attacks that involve long availability of the network.

One case how DOS attack [3] occurs is, by fully depleting the nodes' power. Is is an simple example of a resource depletion attack, where target for attack is bandwidth as resource. This type of attacks where the attacks are done with an aim of depleting the entire resource for causing permanent denial of network service are called vampire attacks.

In this project, it has been considered to study about, how these routing protocols, which are actually designed and developed [4] to be safe and secure are still vulnerable to security attacks and are lacking protection from these attack such as vampire attacks.

Vampire vulnerabilities are not belongs to a particular protocol. They do not depend on the design mechanism or implementation errors. However these attacks try to take advantage of the faults present in the trivial properties of the protocol classes. The classes include link-state, distance vector, geographic routing, beacon routing and source routing. These vampire attacks are not dependant on overflowing the network with huge amount of data, instead they propagate very less data to the possible extent however, and they target the entire exhaustion or draining [5] of the energy in the network. As vampire attacks makes use of the protocol compatible communication (messages) they are highly difficult to identify and restrict.

Different types of vampire attacks can happen in both protocols, i.e., stateless and stateful [6]. In case of stateful protocols, the nodes present in the network know the topology and state of the network. Hence, based on the stored rate they make local forwarding decisions.

In case of OLSR protocols, whenever a new link is enabled or a link goes down, the nodes will store status reports of the links present in the network i.e., whether the link is up or the link is down. Also the nodes keep track of the overflow routing changes whenever the link goes down or established.

Routing in link state and distance vector networks are constructed vigorously from many individual forwarding decisions in a dynamic manner. Hence the adversaries have very little to influence on the forwarding phase of the packet. This makes these protocols [7], i.e., link state protocols to be resistant against the carousel, stretch attacks. The possibility of occurrence of vampire attacks gets reduced to a great extent when the adversaries are not able to specify the full path. But still, the affected nodes i.e., malicious nodes are able to falsify the path mis-forwarding the packets to follow a different path other which, it would choose a normal along path.

When nodes in the network are made to take the forwarding decisions, the vampire will lose most of control it is having over the progress of packet during that forwarding stage. However, this is not a complete solution and they (vampires) are still able to waste a lot of energy by sending again the packet in different positions over the network.

Spurious route discovery is another type of vampire attack on routing protocols mentioned above. There are no of ways for the malicious nodes to generate a noticeable topology change. For example, it can do false claims about the link conditions, i.e., claiming that link is down, or a new link is added to node which is not even exist [8] .

1.2 Problem Motivation

The life period of ad hoc wireless network, especially, that of the sensor network is based upon the node's battery power. In so many of the applications where these networks are involved, recharging or replacing the battery is impossible. Power drainage will lead to the failure of the node and often it will also lead to the damage of entire network. Data losses will also occur. We need an efficient energy utilization scheme to transmit the data packets with the minimum amounts of energy.

But, due to vampire attacks [9] malicious nodes consume more energy than that of the honest node. Hence it is important to mitigate these types of attacks in order to reduce the amount of energy used by each node, and to increase the node's battery life.

1.3Objective

Main objective of this project is to create a secure mechanism which can be used to detect the vampire packets and protects from the forwarding of vampire packets and the formation of such packet inside the node.

1.4 Proposed Approach and Method to be Employed

The proposed methodology to approach and mitigate the problem of vampire attacks involves a sequence of 3 important steps which are given below.

First, thorough evaluation of the weaknesses of existing protocols and routing layers against the resource depletion attacks such as node's battery draining has been done. From that it has been observed that, security schemes to protect Vampire attacks require a different strategy to work compared to utilize for protecting routing infrastructure, and so existing secure routing protocols such as SEAD do not resistant against Vampire attacks.

Second, simulation results are obtained, measuring the functioning of a number of protocols during the presence of a single vampire.

Third is the modification of the present sensor network protocol is done to reduce the damage done by the vampire attacks during the forwarding phase of packets.

In the present work, PLGPa protocol has been used to safe guard against the vampire attacks. This PLGPa protocol attaches the verifiable path history to each and every packet in the network, while maintaining the no backtracking property. This attached path history for every packet is used by PLGPa along with the PLGP's tree routing structure. This way each forwarding node verifies the node signature to make sure that, the packet has followed the correct path and has not traversed away from its target within the logical address space. In this project, we are extending secure transmission by using an efficient key management [10] scheme for sensor networks. The proposed key management methodology is based on the truth that, a sensor communicates only with a small fraction of its neighbors. This decreases the communication and computation expenses of a key setup to great extent. To further improve this methodology of key management, a public key algorithm named Elliptic Curve Cryptography is used in the current work.

2.Literature Survey

As already discussed in introduction, research on these vampire attacks is not adequate and the problems are not yet defined, evaluated, or mitigated in a comprehensive manner at the routing layer [11]. As we know that these vampire attacks are meant for resource depletion i.e., power exhaustion of the nodes batteries. These types of attacks obstruct nodes from incoming into a less power cycle, which is a result of which the batteries will not sleep and will drain really quick compared to normal situations. And the recent research works on the "denial-of-sleep attacks" only judges the attacks that generally happen at the MAC layer. Part from increasing the efficiency of underlying the routing protocols and MAC or switching away from source routing, effective mitigation measures were not proposed in most of the works.

Even in case of systems where power is not constrained, depletion attacks occur by exhaustion of other possessions like CPU time which may affect the network. One simple example for such type of attacks is "SYN flood attack". In this type

attack, adversaries establishes multiple connection requests to server, as a result of which the server will do the allocation of resources for each adversary connection request without knowing that is a malicious attack. These types of attacks can be overcome by keeping the larger weight on the connecting entity. This type of solutions [12] places the small load on the legitimate clients who takes the initiation for stabling small number of connections but it does not the prevent from the malicious entities who will establishes the large number of connections.

Though there is minimal research and information available on vampire attacks and their mitigation measures, there is a good amount of literature available on attacks and diominatingagainst QoS, or RoQ attacks. These types of attacks are responsible for the long-term deterioration in the quality of network performance. The research work on these type of attacks are mainly done on the transport layers instead of the routing layers. Hence, The results and methodologies proposed for these attacks are not suitable for the vampire attacks.

Related work includes study and mitigation measures on DOS attacks in ad hoc wireless network. Most of the work has dealt with attacks which can prevent route setup, interrupt communication, and establishing routes on their own to drop, modify or monitor attack packets.

However, this type of attacks where denial or degradation of service attacks happens to deteriorate the battery life and other limited resources is not a primary consideration, making this research different compared to research on vampire attacks.

The original version [13] of the protocol, i.e., PLGP is designed in such a way to be secure and strong against the attacks. However, the protocol is still prone to vampire attacks because certain drawbacks. PLGP method consists of a series of phases beginning with topology discovery and then packet forwarding. This phase is made to repeat on a predefined plan in order to ensure that most recent i.e., current topology information is present.

2.1 Topology finding phase

Topology finding starts with incomplete period. And during this period, all nodes in the network should declare their existence by distribution an identity certificate. The other things which include during the discovery and broadcasting are its public key, accepted by the trusted party. All nodes will start with their group of size [14] one having a address 0. In cases, where, two individual nodes form the size 2, one of node will accept the address 0, when the other beecomes 1 and it is shown in the below figure1.

2.2 Packet forwarding phase

Through the forwarding phase, each decision is made by every node independently makes all the decisions that are needed. When receiving packet, node finds the next node by inventing the MSB bit of its address which is different from the source's address. In that manner, each forwarding event decreases the logical distance to the final end point or target, as node's address must be exactly closer to the target.

2.3 Issues in the Existing PLGP system

There are so many drawbacks in the existing PLGP system which are as follows.

- Outage of power events
- Environmental disasters and loss of information.
- Security level is poor
- Prone to several DoS attacks.
- Productivity losses due to lack of access to network
- Attacks that affect the availability for long-term are not addressed.

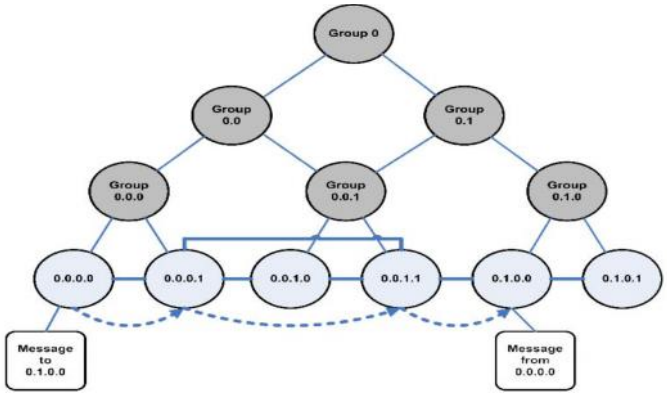

Figure1: address of tree in the network

3. Proposed Approach

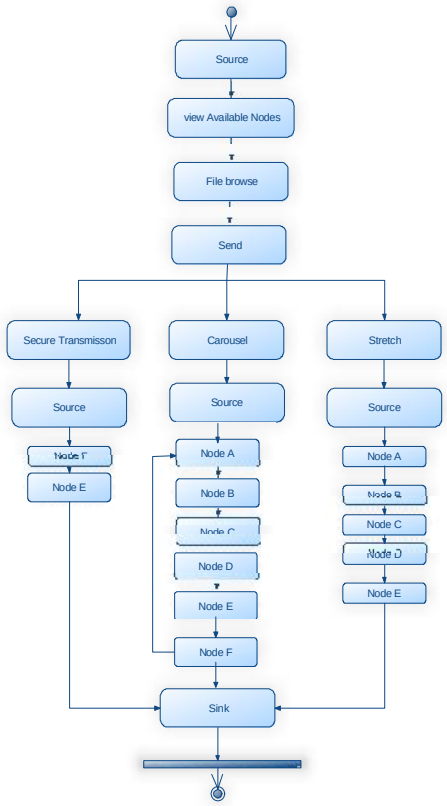

Figure2: Process of proposed approach

3.1 Implementation

We have implemented the project with the following modules

- Network Creation Module
- Carousel attack Module
- Stretch attack Module
- Energy Level Identification Module
- Secured Transmission Module

Network Creation Module: We have created the network with source, sink and six nodes named A, B, C, D, E, F. Each node is having a unique identification number and topology discovery is done at transmission time. Transmission of data is possible based upon the malicious nodes and honest nodes. If any malicious node is present in our network nodes then it will chooses the longest path or loops. We need to the fix the malicious node in the network otherwise it will corrupts the entire network nodes to be deployed and cannot control their positions.

Carousel attack Module: In this attack, malicious node composes the packets with purposely by introducing the routed loops. This is called as a carousel attack and it forwards the packets in the path form in the below figure. In these attacks, same node occurs so many times while routing the packet in the network. Mainly this attack is used to raise the length of the route.

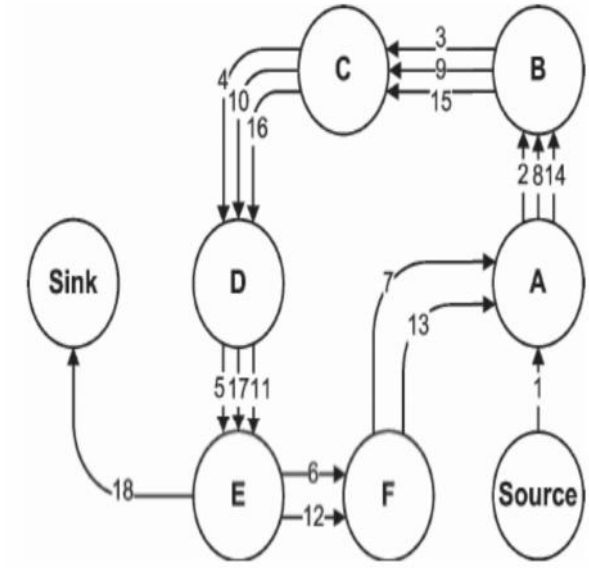

Fig 3: carousel attack

Stretch Attack Module: In case of stretch attack, the adversary itself creates long paths by mainly traversing each and every node in the network. It increases the packet path lengths and it is shown in the figure. In a randomly generated topology, Carousel attack increases the energy consumption by a factor of 4, stretch attacks increments the usage of energy and it depends upon the malevolent node.

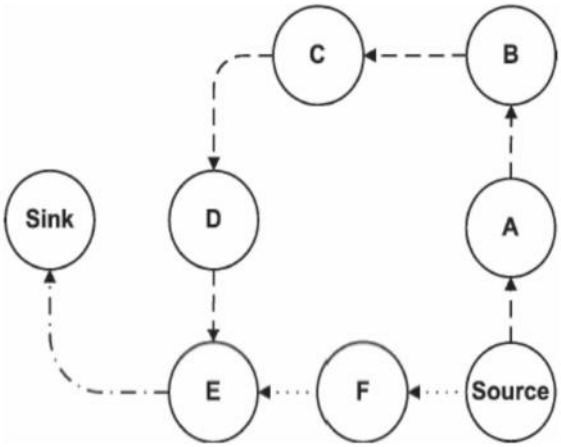

Figure 4: Stretch Attack

Energy Level Identification Module: In this module, we show the energy levels for each and every node to demonstrate the vampire attack affect. Here, node is permanently stops working once the bandwidth of the node are exhausted. Nodes can be recharged by active cycles. During frequent charging cases, power exhausting attacks are more dangerous if the adversary consumes more power rather than the nodes can recharge. Vampire attacks many honest nodes if the sending packet constitutes amplification.

Secured Transmission Module: In this module, we protect the nodes bandwidth and network from vampire attacks by sending the secured transmission. In this secured transmission data travels in the honest node and mitigates the vampire attack during the packet forwarding phase.

3.2 ECC Algorithm

Electric curve cryptography is a public key cryptography. ECC protection depends upon the ability to determine the point multiplication and inability to determine the multiplicand with the novel and production points. Difficulty of the problem is based upon the elliptic curve size.

Primary advantage of using the ECC is to reduce the storage, smaller key size and transmission requirements.

For the existing cryptographic schemes, an **elliptic curve** is plane curve over the finite field. It contains the points which are used to satisfy the below equation.

$$y^2 = x^3 + ax + b,$$

The basic operations of ECC are Point Multiplication, Point Addition and Point Doubling.

3.2.1 Point Multiplication

Q = KP

Example: consider K= 28

Q = 28 P = 2(2 (2 ((P + P) +P) +P)) + P

3.2.2 Point Addition

Point addition is used to add the point say P and Q for getting different point say R on the same curve.

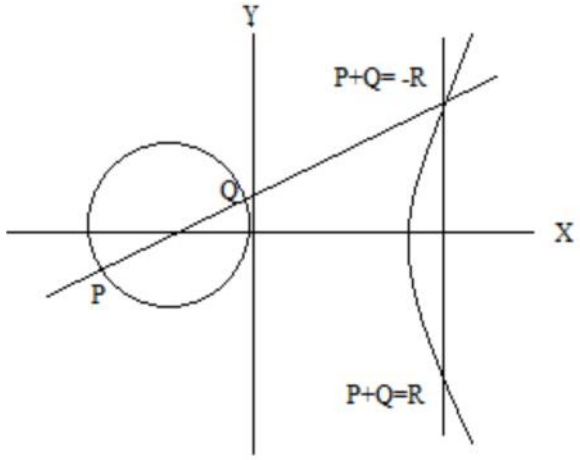

Figure5: Point addition

3.2.3 Point Doubling

Point doubling is the summation of the point P to itself to get different point on the same curve.

So R = P+P =2P

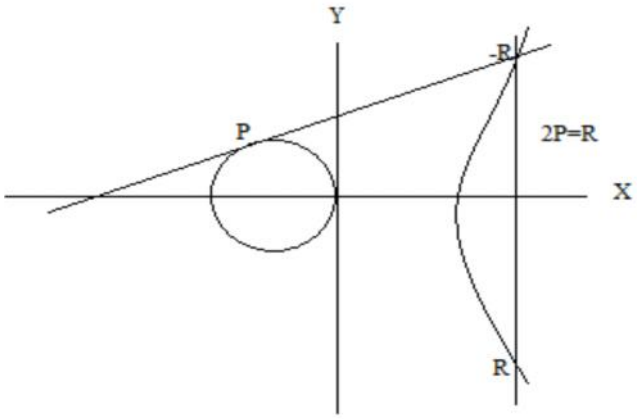

Figure6: Point Doubling

4. Conclusion and Future Scope

4.1 Conclusion

Following conclusions were made during the course of this project work.

- Vampire attacks are defined and understood as a new class of attacks that are responsible for causing complete exhaustion of the network resources by draining the nodes battery power, thereby causing the permanent Denial of Service.
- Vampire attacks are not definite to specific protocols and also do not depend on specific implementations.
- These attacks depict the weaknesses of WSNs in several major protocol classes.
- Representation of these attacks on a modeled i.e., representative environment of a routing protocols has been done using a small no of weak adversaries.
- The measurement of those attacks has also been done to understand the effect of these attacks on the network, and to understand the effectiveness of the proposed methodology to secure the WSN from vampire attacks on a accidentally generated topology.

To safeguard such attacks, defense measures were proposed in the form of PLGP protocol.

4.2 Future Scope

The solution offered in the present work is working but not a comprehensive and complete satisfactory solution for protecting the WSNs against Vampire attacks during the topology finding phase. However, the proposed method has given some idea about how damage limitation can be done with further changes to the existing PLGPa. It protects from the affects and military protection for handling the mobile networks, as well as for topology discovery, is left for future work.

5. References

[1] I. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. ACM MobiCom, 2004.

[2] 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, Nov. 2006.

[3] T. Aura, "Dos-Resistant Authentication with Client Puzzles," Proc. Int'l Workshop Security Protocols, 2001.

[4] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.

[5] D. Bernstein and P. Schwabe, "New AES Software Speed Records," Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), 2008.

[6] D.J. Bernstein, "Syn Cookies," http://cr.yp.to/syncookies.html, 1996.

[7] I.F. Blaked, G. Seroussi, and N.P. Smart, Elliptic Curves in Cryptography, vol. 265. Cambridge Univ. , 1999.

[8] J.W. Bos, D.A. Osvik, and D. Stefan, "Fast Implementations of AES on Various Platforms," Cryptology ePrint Archive, Report 2009/ 501, http://eprint.iacr.org, 2009.

[9] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

[10] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

[11] J.-H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol. 12, no. 4, pp. 609-619, Aug. 2004.

[12] A.J. Goldsmith and S.B. Wicker, "Design Challenges for Energy-Constrained Ad Hoc Wireless Networks," IEEE Wireless Comm., vol. 9, no. 4, pp. 8-27, Aug. 2002.

[13] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom, 2002.

[14] M. Maleki, K. Dantu, and M. Pedram, "Power-Aware Source Routing Protocol for Mobile Ad Hoc Networks," Proc. Int'l Symp. Low Power Electronics and Design (ISLPED), 2002.

ISSN 2321-6905

Authors

Pavani Potnuri received the Bachelor's Degree in Information Technology from NOVA Engineering college affiliated to JNTUH. She is received her master's degree in Computer Science and Engineering from SAARADA Engineering college affiliated to JNTUH. Now she is working as Assistant Professor in Amrita Sai Institute of Science & Technology. Her research areas are Data Mining and Software Engineering.
Email id: pavani_875@yahoo.co.in

Gowru Bharath Kumarreceived the Bachelor's Degree in Information Technology from Bapatla Engineering College in 2008-2012. He is received him master's degree in computer science and technology from V R Siddhartha Engineering College. Now he is working as Assistant Professor in Amrita Sai Institute of Science& Techonology. His Research areas are Data Mining, Text Mining and Web Mining.
Email id: bharath.kumar436@gmail.com

Venkateswara Rao Nadakuditi received the Master's degree from Amrita Sai Institute of Science & Technology. Now he is working as Assistant Professor at Amrita Sai Institute of Science & Technology. His research areas are Data Mining and Computer Networks.Email id: n.venkat056@gmail.com