VAMPIRE ATTACKS IN WIRELESS SENSOR NETWORKS: EVALUATION AND PROTECTION

[1]Farheen Fatima, [2]L Sunitha, [3]E.Venkata Ramana

[1,2,3]Department of computer Science and Engineering, Vidya Vikas Engineering College, Ranga Reddy, India

Abstract: **A vampire attack is caused by the malicious node on the decentralized ad hoc wireless network. The paper analyses how protocols faces these attacks. Vampire attacks are not protocol specific rather uses its compliant message. The current security measures to prevent these attacks are been reviewed along with result of simulation of representative protocols in the presence of a vampire attack is been presented. The paper also describes how the existing sensor network protocol is been modified for protection from the vampire attacks for which PLGP solution is also been proposed.**

Keywords: **ad hoc, protocol, carousel attack, stretch attack, PLGP.**

I. INTRODUCTION

Ad hoc wireless sensor network consists of various sensors that are expanded in a space where each sensor performs signal processing and data networking providing operational efficiency. The ad hoc wireless servers are self-organized and energy constrained. These sensor networks are used to detect information of enemy base, monitor environmental changes and are also used for security purposes in various places like shopping and parking arena. When these networks face attacks causing negative effect by causing battery exhaustion and higher energy utilization.

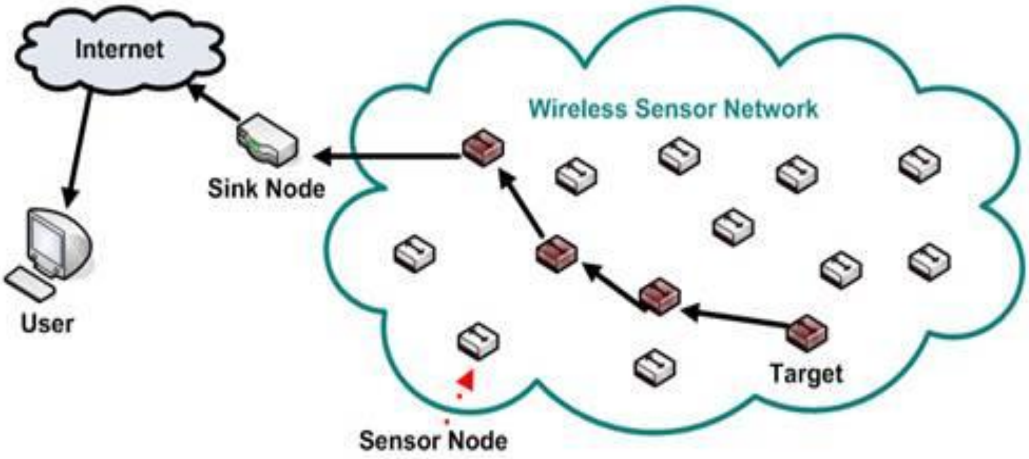

Fig 1: Ad hoc Wireless sensor network

Vampire attacks are caused when a message is been initiated and transmitted through a malicious node over the network causing higher battery utilization and battery exhaustion. Vampire attacks are not constrained to a specific type of protocol and does not alter specific path in the network. When a network is been attacked by them, even transfer of small data consumes more energy.

II. CURRENT SECURITY MEASURES

Wireless ad hoc sensor networks have been one increasingly adopted network due to various advantages it has been providing, but vampire attacks have ben emerging as one major threat to these networks. Instead of security measures applied, the networks are still susceptible to vampire attacks. Some of the methods applied are:

1. One way hash chains are applied to prevent these attacks which are usually caused over a path in the network that transmits the data packets. These chains prevent attacks by restricting the rate at which these packets are transmitted. As this technique can be applied to only limited networks, it is not recommended.
2. Ad hoc on demand distance vector routing is another technique applied which trust threshold value is been applied to the effected node depending on which the affected node is been eliminated.
3. For routing infrastructure, the transmission can take place utilizing minimum energy for transmission and receiving of packets using an energy aware routing protocol.

Many other methods are also applied which include loose source routing, many other security protocols, rushing attack prevention protocol, packet leash technique etc. However these methods have their drawbacks as these cooperative node behaviour which cannot prevent vampire attack to occur.

III. TYPES OF VAMPIRE ATTACKS

There are two type of protocols prone to vampire attacks that are identified:

a. Stateless Protocol: In this protocol, the initial node caries the address of the direction to be followed to reach the destination node. These protocols make systems robust but are prone to attacks.

b. Stateful Protocol: These protocols make decision for flow of data when in stored state and are also prone to attacks.

There are four different types of attacks on these two protocols.

1. Carousel attack: The stateless protocols are prone to this kind of attacks. These attacks lengthen the route and causes lesser verification of message header from where the message has to pass on.

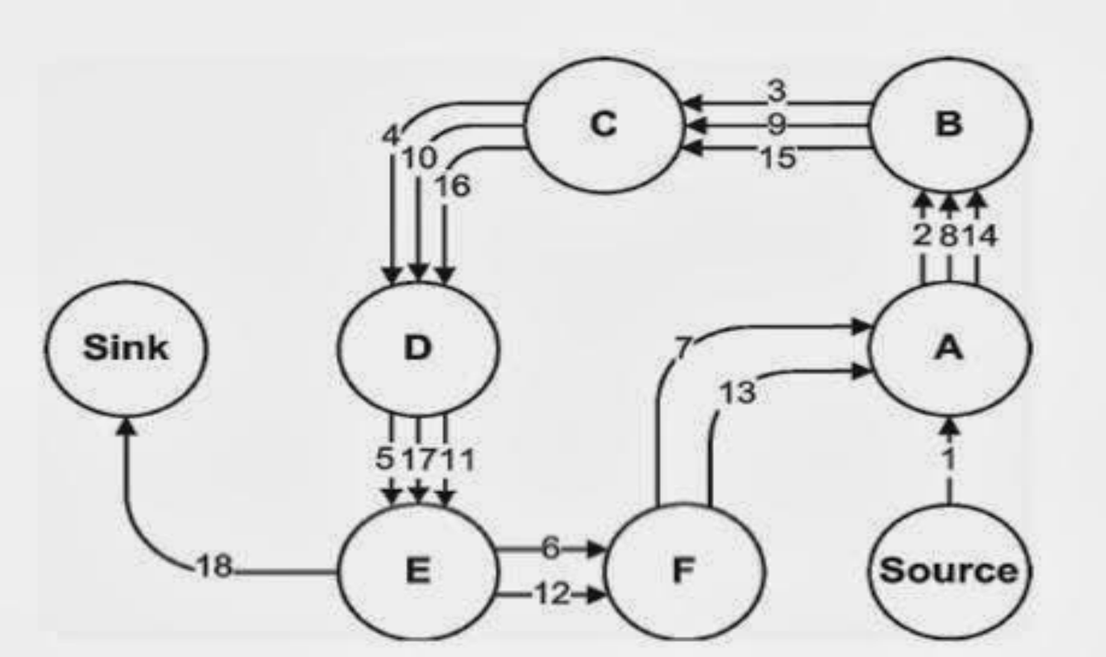

Fig 2: Carousel Attack

2. Stretch attack: These attacks are also caused on a stateless protocol. These attacks stretches the number of nodes in the path and creates artificial long routes.

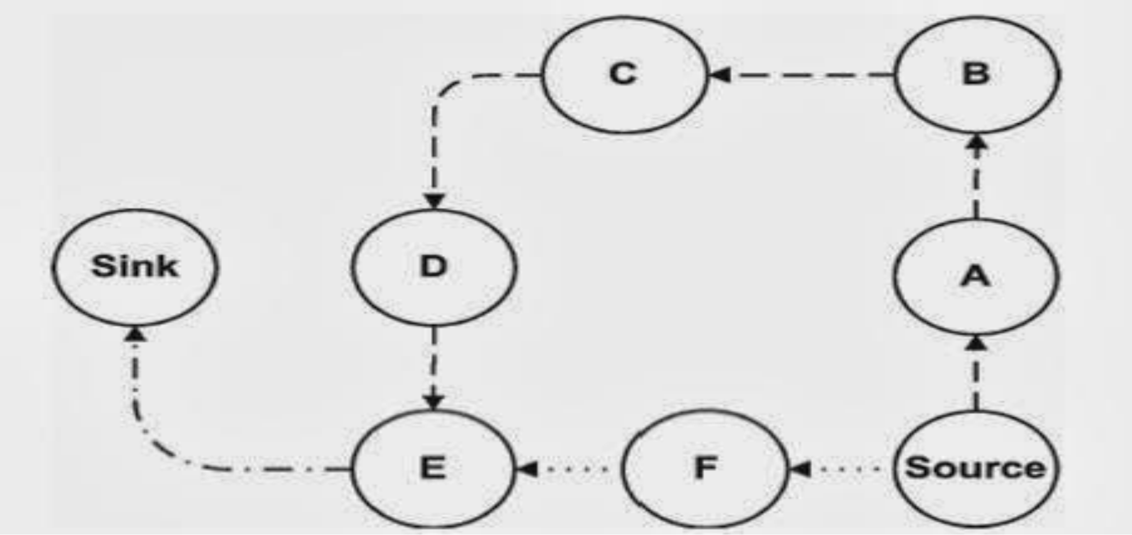

Fig 3: Stretch Attack

3. Directional Antenna Attack: The stateful protocol are prone to these attacks. This causes additional energy consumption at the source node and also consumes energy of the nodes that are not part of the path for packet transmission

4. Malicious Discovery Attack: This attack also directs towards stateful protocol. In these attacks an error is created stating the link does not exist and a new non-existent link is been made.

IV. SIMULATION RESULT

We can consider time consumed during denial of service and at honest node. If a denial of service node takes 10 minutes of the time in transmitting data packet, honest node utilizes only 10% of that time to carry out similar task. Simulation results for these can be noted by analysing fraction of node energy consumed against fraction of total nodes.

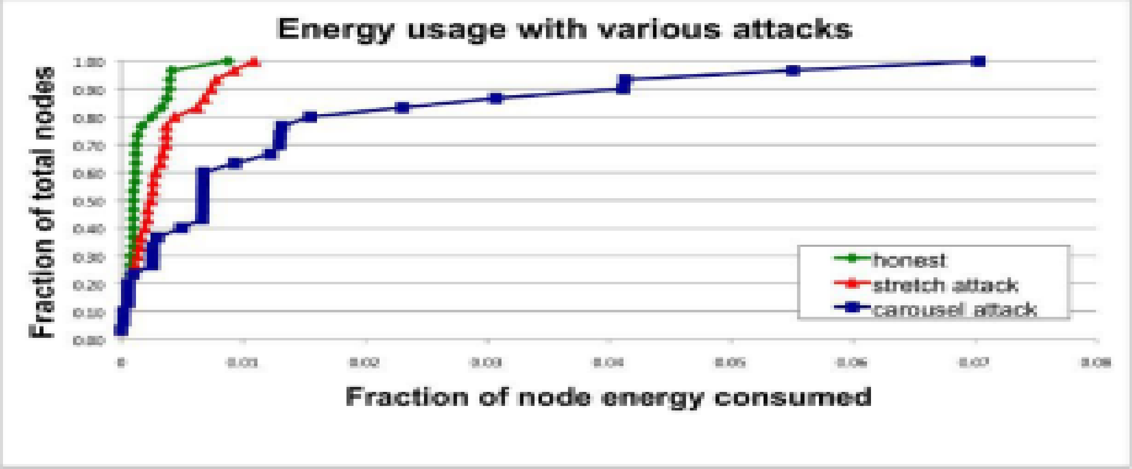

Fig 4: Result of packet transmission under attacks

V. SECURITY AGAINST VAMPIRE ATTACKS

A Clean Slate Sensor Network Routing by PLGP (Parno, Luk, Gaustad and Perrig) can be applied which consists of two phases:

i. Topology Discovery Phase
ii. Packet Forwarding Phase

I. Topology Discovery Phase:

A node starts with its virtual address as zero. At each node a certificate is been issues which contains the public key for identification. Each node is connected to the other and shares virtual address, public key and the certificate when they merge with closest nearby group.

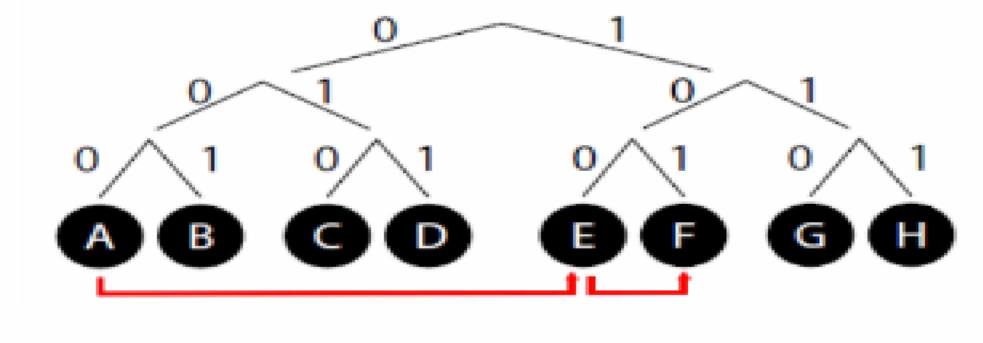

Fig 5: Topology Discovery Phase

II. Packet Forwarding Phase:

The packets are forwarded in this phase as shown in figure 6.

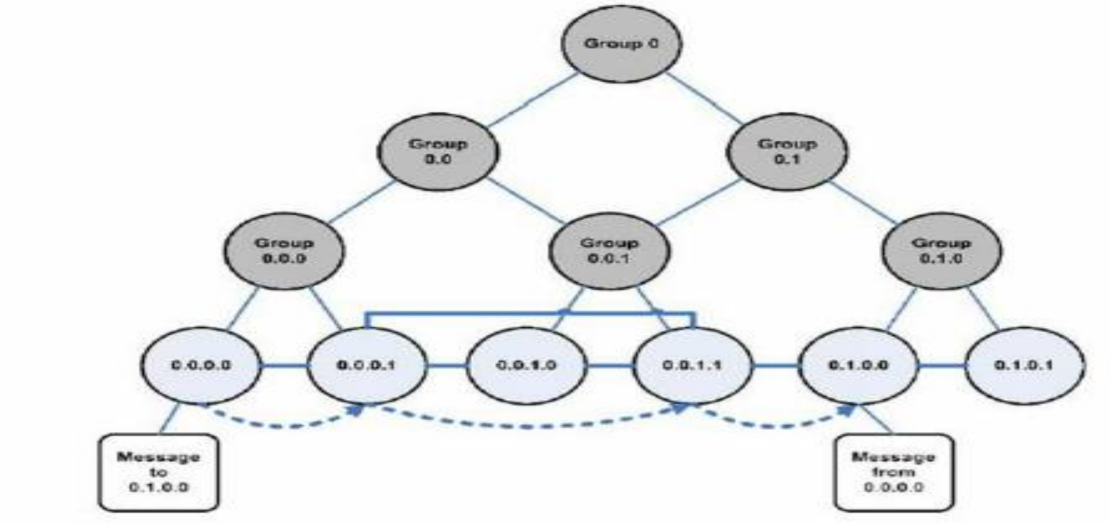

Fig 6: Packet Forwarding Phase

PLGP proposed a solution which suggests:

a. Providing a verifiable path history to all the packets involved.

b. Using this path history the packet transmission can take place through every node securely passing through at least one honest node.

c. Each node upon receiving the message, checks for authentication in the chain.

VI. CONCLUSION

Vampire attacks have been the kind of attack that effects the wireless ad hoc sensor networks using the protocols to disable them and consuming high amount of energy. These attacks does not depend on particular type of protocol. Ad hoc network sensors have been applied in various fields which needs to create and identify solutions for prevention of the network from these attacks. There are different types of vampire attacks depending on the protocol. When the attack take place it not only consumes higher power but also takes additional time. There are many solutions and techniques that have been presented to prevent these attacks but were not effective enough which creates a need for a better solution. PLGP solutions can be applied to these protocols in order to prevent these networks that are often prone to vampire attacks.

REFERENCES

[1]. Deng. J. Han. R. and Mishra. S. “Defending against Path-Based DoS Attacks in Wireless Sensor Networks”, proc.ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.

[2]. Doshi. S. Bhandare. S. and Brown. T.X. “An On Demand Minimum Energy Routing Protocol for a wireless Ad Hoc Network,” ACM SIGMOBILE mobile computing and communication. Rev. vol. 6, no. 3, pp, 50-66, 2002.

[3]. Douceur. J.R.”The Sybil Attacks”, proc. Int’l Workshop Peer-to-Peer Systems, 2002.

[4]. Feency. L.M. “An Energy Consumption model for Performance Analysis of Mobile Ad Hoc Networks,” mobile Networks and Applications, vol. 6, no. 3, pp. 239-249, 2001.

[5]. Goldsmith. A.J. and Wicker. S.B. “Design Challenges for Energy Constrained Ad Hoc Wireless Networks”, IEEE Wireless Comm., vol. 9, no. 4, pp. 8-27, Aug. 2002.
Jae-Hwan Chang and Leandros Tassiulas, Maximum lifetime routing in wireless sensor networks, IEEE/ACM Transactions on Networking 12 (2004), no. 4.

[6]. Hans Eberle, Arvinderpal Wander, Nils Gura, Sheueling Chang-Shantz, and Vipul Gupta, Architectural extensions for elliptic curve cryptography over GF(2m) on 8-bit microprocessors, ASAP, 2005.

[7]. INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications 29 (2006), no. 2.

[8]. Jing Deng, Richard Han, and Shivakant Mishra, Defending against pathbased DoS attacks in wireless sensor networks, ACM workshop on security of ad hoc and sensor networks, 2005.

[9]. John R. Douceur, The Sybil attack, International workshop on peer-topeer systems, 2002.

[10]. Johnson. D.B. Maltz. D.A. and Broch. J. “DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networking, Addison-Wesley, 2001.

[11]. Karlof. C. and Wagner. D. “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Proc. IEEE lnt’l Workshop Sensor Network Protocols and Applications, 2003.

[12]. Karp. B. and Kung. H.T. “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks”, pro. ACM MobiCom, 2000.

[13]. Laura M. Feeney, An energy consumption model for performance analysis of routing protocols for mobile ad hoc networks, Mobile Networks and Applications 6 (2001), no. 3.

[14]. Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, Strong authentication for RFID systems using the AES algorithm, CHES, 2004.

[15]. Park. K. and Lee. H. ”On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attacks,” proc. IEEE INFOCOM,2001.

[16]. Raffo. C. Adjih. T. Clausen, and P. Muhlethaler, “An Advanced Signature System for OLSR”, pro. Second ACM Workshop Security of Ad Hoc and Sensor Networks, 2004.

[17]. Rodrigo Fonseca, Sylvia Ratnasamy, Jerry Zhao, Cheng T. Ee, David Culler, Scott Shenker, and Ion Stoica, Beacon vector routing: Scalable point-to-point routing in wireless sensornets, NSDI, 2005.

[18]. Sheetalkumar Doshi, Shweta Bhandare, and Timothy X. Brown, An ondemand minimum energy routing protocol for a wireless ad hoc network, ACM SIGMOBILE Mobile Computing and Communications Review 6 (2002), no. 3.

[19]. T. English, M. Keller, Ka Lok Man, E. Popovici, M. Schellekens, and W. Marnane, A low-power pairing-based cryptographic accelerator for embedded security applications, SOCC, 2009.

[20]. Thomas H. Clausen and Philippe Jacquet, Optimized link state routing protocol (OLSR), 2003.