I J C T A, 8(5), 2015, pp. 2051-2061

Surveying the Effect of Vampire Attack in Wireless Ad-hoc Sensor Networks

R. Isaac Sajan*, J. Jasper and E. Arun*****

Abstract: Ad-hoc low power wireless networks are composed of few to large number of sensor nodes. The energy resources provided for these sensor nodes will be limited. This paper explores a type of resource depletion attacks at routing protocol layer, which are termed as vampire attacks. Vampire attacks are difficult to detect, but easy to carry out. The worst case scenario is that, a single vampire can increase network-wide energy usage by a factor of O(N), where 'N' is the number of nodes in the network. In this paper, we make a study with the use of PLGP protocol, which consists of topology discovery and packet forwarding phases and both the phases are prone to vampire attacks. A protocol named PLGPa was implemented with modification that resists the vampire attacks during the packet forwarding phase and in topology discovery phase. This protocol makes use of signature and attestation chains in order to verify that the packets consistently make progress towards destination during transmission.

Key Words: Wireless networks, sensor nodes, attestation chain, resource depletion.

1. INTRODUCTION

Wireless sensor networks are a note worthy category of networks which provides wireless communication infrastructure in the midst of sensors deployed in a distinct application domain. A sensor network is a group of large number of sensor nodes that are placed in a specific region. Sensors use low power and have limited memory. They uses energy in a constrained way due to their small size. Wireless networks can also be deployed in extreme environmental conditions and may be prone to enemy attacks. They need to be self-organized and self-healing and can face constant reconfiguration.

Wireless ad-hoc sensor networks are decentralized type of wireless sensor networks. Such networks are said to be ad-hoc because it does not depend on any pre-existing infrastructure such as routers in wired networks and access points in managed wireless networks. Here, all the devices possess equal status and every node participates in routing by forwarding packets. Wireless ad-hoc sensor networks are already used to monitor environmental conditions, factory performance and troop deployment. In the near future, wireless ad-hoc sensor networks promises new applications such as continuous connectivity, ubiquitous on-demand computing power, instantly deployable communication for military and first responders.

Availability is an important constraint when designing networks. Most of the attacks such as Denial of Service (DoS), Black-hole attacks, Worm-hole attacks, Sybil Attacks etc. are targeted on disrupting the availability. The existing security works are focused mainly on denial of communication at routing or MAC levels.

2. LITERATURE SURVEY

We don't express that draining of power is different, but instead these attacks are not defined and evaluated in the routing layer. A term "sleep deprivation nature[2] is mentioned in early methods, which means this

* Research Scholar, Ponjesly College of Engineering,Nagercoil, KK Dist,629001,India. *Email: ponjeslyisaac@gmail.com*

** Professor, Department of Electrical and Electronics Engineering, Ponjesly College of Engineering,Nagercoil, India. Email: mailtojasper@gmail.com

*** Professor, Department of Electronics and Communication Engineering, Ponjesly College of Engineering, Nagercoil, India. *Email: drearun@yahoo.com*

attack does not allow the nodes to enter a low-power sleep cycle and typhus the battery power is drained faster. But new research on “denial-of-sleep” considers the sleep cycle only at the MAC layer[3]. Other research work mentions the power draining at the MAC and transport layers[4, 5, 32]. The malicious routing loops are explained [6, 7] but no preventive measures are undertaken. Instead, the efficiency of the MAC and the routing protocols are increased or switched away from the source routing.

In power-confining systems, the consumption of memory, processor power and bandwidth cause some problems. A familiar example is the SYN flood attack in which the adversary will make several connections request to the server and the server will allot the resources for each request. Thus the resource gets depleted. But the adversary who allocates minimum resources remains operative. Such attacks can be reduced by imposing more burden on the connection establishment (Example., SYN cookies[8] which reduce the initial connection state in the client or cryptographic puzzles[9, 10, 11].These solutions provide minimum load on the legal client who request minimal connection request but prevent the client with large number of connection. This is a type of rate limiting but, it is not preferable because it punishes the nodes that produce heavy traffic but does not send more data on the network. Since vampire attack depends upon amplification, these solutions are not effective to explain about the excess load on the legal nodes.

There are previous research work that describes the attack on quality of service (QoS) depletion in the network performance[12, 13, 14, 15, 16, 17, 18]. These papers focus on the transport layer instead of routing protocols. Since, vampire attack do not drop the packets, the quality of the path remain high with increased latency. Other literature on denial of service in ad hoc networks is expressed with adversaries who forbid the route setup, interrupt communication or establish own routes to drop and monitor the packets[19, 20, 21, 22, 23]. The effect of denial of service on battery power and other resources are not considered for security. Protocols that express security in terms of path routing success cannot be protected against the vampires, since these attacks do not use illegal routes for communication. The proposed work in minimum energy routing focus on the increase of lifetime of power –confining network by using low energy for the transmission and reception of packets (eg., by minimizing the transmission distance)[24, 25, 26, 27] is orthogonal. These protocols focus on the cooperative nodes instead of malicious nodes. Additional works on power–consuming MAC, cross–layer cooperation and upper layer protocols have been proposed. However, the vampire attack will increase the energy usage in minimum energy routing outline and when the power consuming MAC protocols are used, these attacks cannot be avoided in MAC layer or in cross–layer feedback. Attackers will generate packets which produce multiple hops than normal so that nodes spend more resource to transmit the packet and make each packet more expensive in the presence of vampires.

Our work proposes an attack –resistant minimum –energy routing which includes energy consumption. Deng et. al explains the path based attack in [28], which includes the rate limiting of nodes to transmit the packets. As an example, Aad et. al explains how protocol complaint nodes degrade the performance of nodes[29, 30]. Thus, they either generate message when legal nodes does not or transmit packets along protocol headers that is different from the legal nodes.

2.1. Features of Vampire Attacks

The major feature of vampire attack is that the network will not get immediately unavailable. Vampires uses protocol compliant messages and transmit data with largest energy drain. Hence, detection of these attacks are difficult, but it can be carried out with less effort. Vampire attacks are not specific to any protocol, but it relies on the properties of many popular classes of routing protocols.

Based on the type of protocols used, vampire attacks of different types can be employed. The routing protocols are either stateless or stateful based on their behavior and functionality. Stateless protocols are certain classes of communication protocols which handles each request as a discrete transaction. Independent pairs of request and response are used in communication, since each transaction is independent of previous requests. There is no need for the server to retain session information when stateless protocols are used. Stateful protocols require the preservation of internal state on the server[8].

2.1.1. Attacks on Stateless Protocols

Stateless protocols are susceptible to two kinds of vampire attacks such as carousel attack and stretch attack. In carousel attack, attacker targets on draining out residual energy of nodes by purposely inducing loops. In the case of stretch attack, malicious routes are formed by elongating the path for traversal.

a) **Carousel Attack**: Carousel attacks are those energy draining attacks by which, attacker creates and transmits packets through routing loops which are purposely introduced[26]. It exploits the limited verification of message headers by the source routing protocol. This allows a packet to traverse through a set of nodes repeatedly and thus forms a loop. This increases the length of route. The increased length is much higher than the number of nodes in the network.

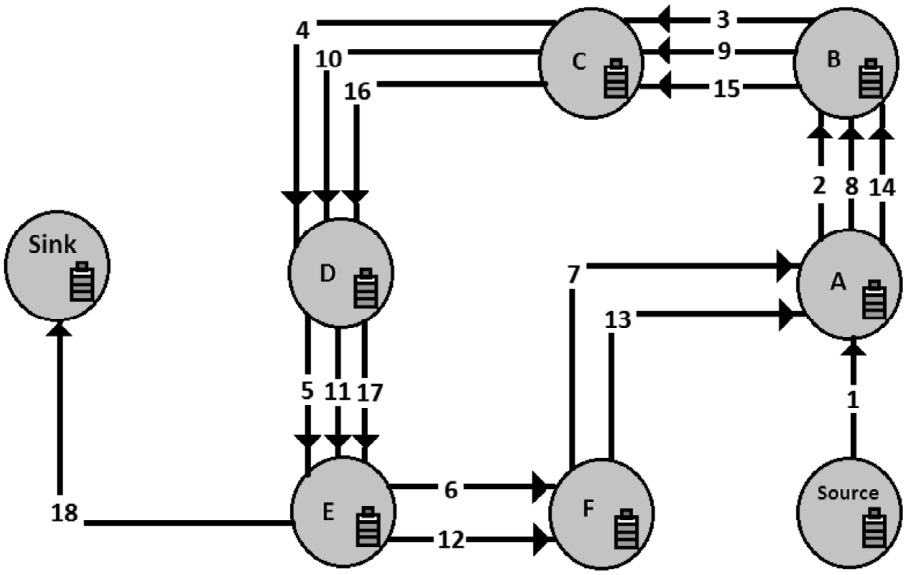


Figure 1 Carousel Attack

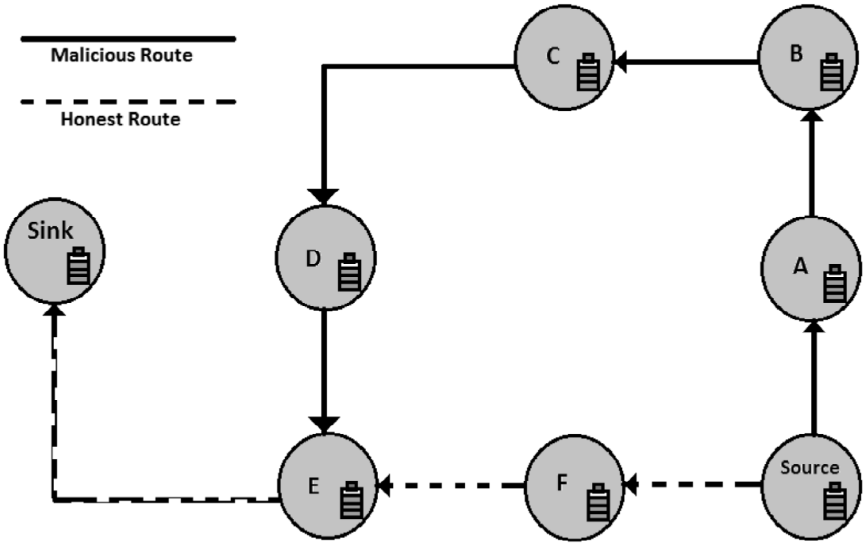


Figure 2: Stretch Attack

A typical carousel attack scenario is illustrated in Figure 1[26]. Here, the packets traverses through the loop with multiple times A-B-C-D-E-F-A, which results in 18 discrete transactions.

b) **Stretch Attack**: Stretch Attacks are those energy draining attacks by which artificially long routes are constructed by malicious node that leads to the packets to traverse a larger number of nodes than the optimal number of nodes. Figure 2[26] illustrates stretch attack. Source—F—E—Sink is the honest route. Here malicious node selects a longer route and it affects all nodes in the network. These path elongation attacks does not have much effect when the network contains small number of nodes, but have a considerable effect in energy consumption when there are hundreds and thousands of nodes in the network[26].

2.1.2. Attacks on Stateful protocols

Stateful protocols consists of two important classes namely link-state and distance-vector. Up/down status of links in the network are maintained in each node, in the case of link-state protocols like OLSR. Whenever a new link is enabled or a link goes down, link-state protocols floods routing updates. In the case of distance-vector protocols like DSDV, route cost metric, e.g. number of hops, is indexed with the next hop to every destination. Stateful protocols are immune to carousel and stretch attacks, since they uses dynamically derived routes with the help of numerous independent forwarding decisions. The power of adversaries are limited due to this reason. The major types of attacks prevalent on stateful protocols are directional antenna attack and malicious discovery attack[8].

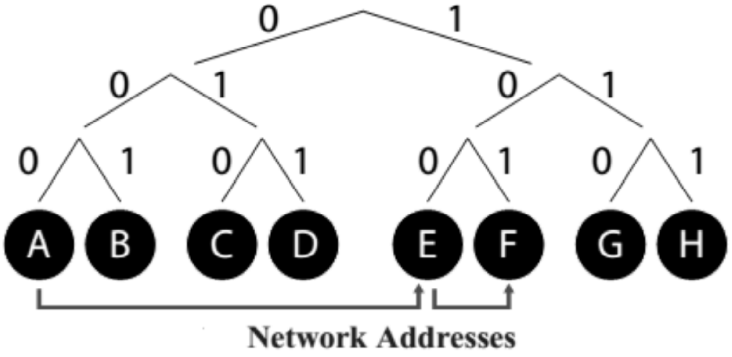
a) **Directional Antenna Attack:** When forwarding decisions are made independently by each node then vampires have small control over packet progress but they can still waste energy by restarting a packet in various parts of the network. Using a directional antenna, in any parts of the network attackers can insert a packet, also while forwarding the packet locally. It uses the energy of nodes that would have to process the original packet, with the expected honest energy expenditure of O(d), where 'd' is the diameter of network. This attack can be said as a half wormhole attack, as directional antenna constitutes a private communication channel. It can be performed more than once by inserting the packet at various distant points in the network, at the additional cost to the attacker for each use of the directional antenna.

b) **Malicious Discovery Attack:** In common routing protocols, route discovery packets are forwarded by every node in the network, and this helps to initiate flood by sending single message. Malicious node activates topology change using a number of ways. It may wrongly claim that a new link added or a link is down to a non-existent node. This attack is trivial in the case of open networks with unauthenticated routes because a single node can make wrong claim about neighboring nodes and can emulate multiple nodes in neighbor relationships.

3. PROPOSED SYSTEM

PLGP protocol uses clean slate sensor network routing[8]. PLGP defends against all sorts of malicious attacks except vampire attacks.

PLGP tree shown in Figure 3 [23]will be constructed after topology discovery phase. Routing table will be constructed on each node, based on PLGP tree. Routing table in node(A) is also shown in Figure 3. Hash tree shown in Figure 4 is constructed by hashing the roots of two sub-trees to form the root of new sub-tree. Recursive grouping is done with the help of hash trees. During recursive grouping, smaller groups repeatedly merges to form larger groups. Leaf nodes represent node-ids and internal nodes represent group-ids. PLGP protocol is vulnerable to vampire attacks, both in topology discovery phase as well as packet forwarding phase. During packet forwarding using PLGP protocol, an attacker can modify hash chains and this results in various vampire attacks such as carousel, stretch etc. These attacks can be prevented using PLGPa



Prefix	Next hop
1.*	E (1.0.0)
0.1.*	C (0.1.0)
0.0.1	B (0.0.1)

A's Routing Table

Figure 3: Routing Table Formation using PLGP Tree

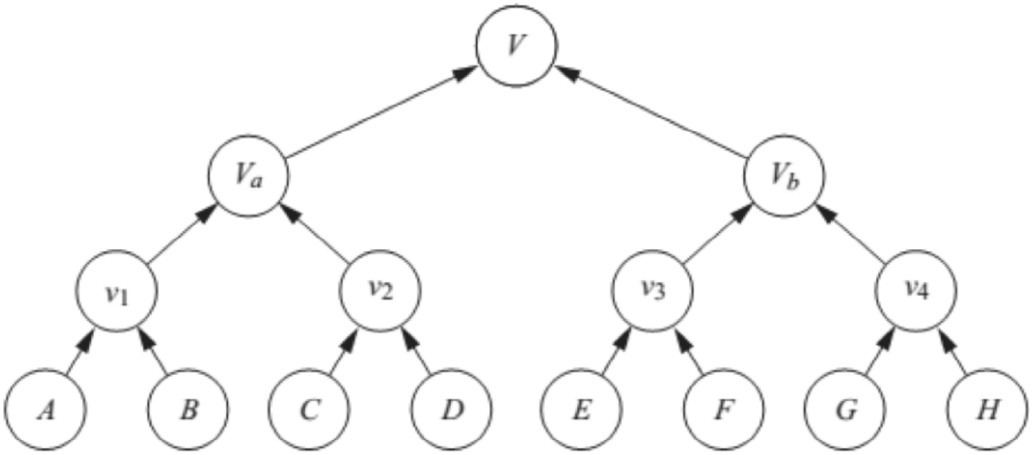


Figure 4: Hash tree formation

protocol by modifying PLGP protocol by incorporating one-way attestation chains [8]. One-way attestation chains permits only append operations at a single end. This enables no-backtracking property. Thus vampire nodes can be detected by analyzing the entries appended on attestation chain. Path elongations and loops can be detected at each node by verifying attestation chains.

A secure packet forwarding mechanism can be implemented by guaranteeing that the packets will continuously make progress towards destination during packet forwarding. Packets cannot make progress when there is no alternate valid path with no vampire nodes. In such cases, packets will be dropped to avoid further congestion and energy loss. If the neighbor specified in attestation chain is not present, the packet gets forwarded to the next hop of non-neighbour.

4. PERFORMANCE EVALUATION

The performance of the implemented system can be analyzed with the help of x-graph utility for generating 2-D graphs. The values for analyzing performance can be retrieved from trace files obtained during simulation using AWK scripts.

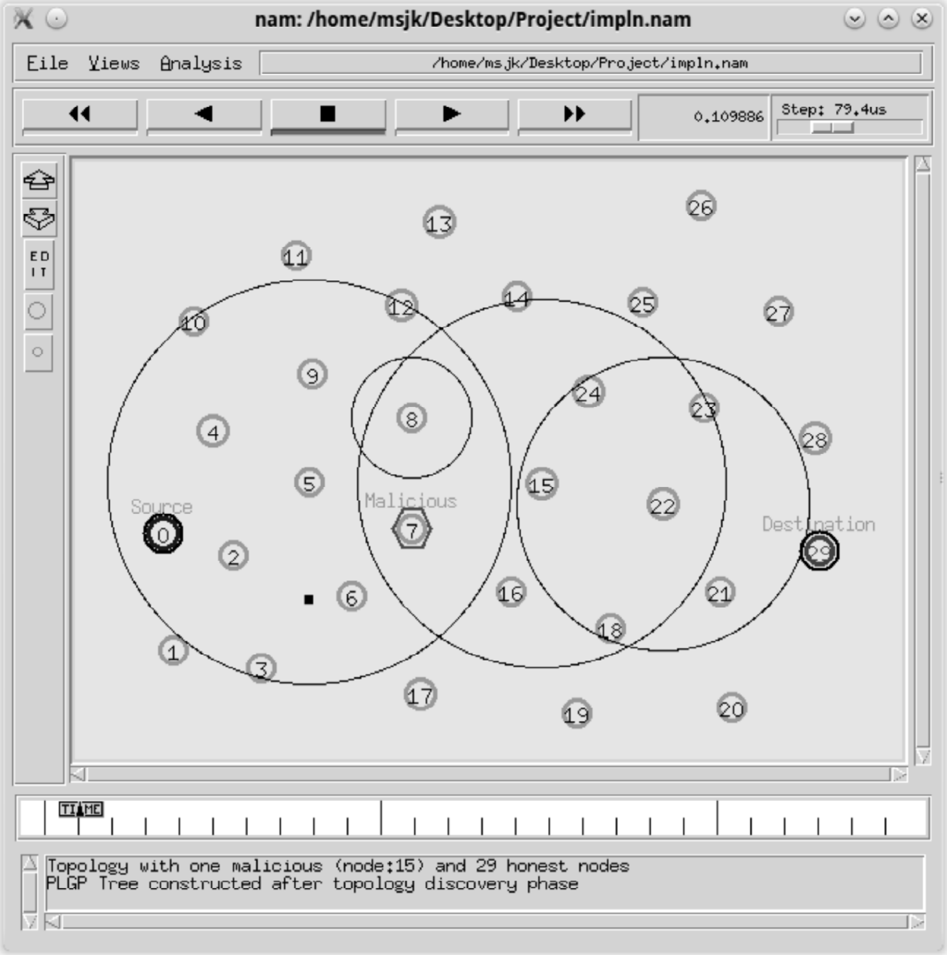
4.1. Simulation Setup

The simulation was carried out using ns2 simulator, by creating a 30-node flat-grid topology, out of which, one node is vampire node. A series of simulations are conducted in order to compare the performances of existing PLGP protocol and the proposed PLGPa with modification protocol. IEEE 802.11 was taken as the MAC sub-layer protocol. 914 MHz Lucent WaveLAN radio interface with maximum attainable bandwidth of 2 Mbps was set upped along with a unity gain, 1.5m height Omni-directional antenna. Sensing range was taken as 50m and communication range was taken as 250m. An energy model was created for each and every node in the topology. Energy model consists of parameters such as initial energy, transmission power, reception power, idle power and sense power. Each node possesses 5 joules of energy during the initial stage. Transmission power was set as 1W, reception power was set as 0.5W, idle power was set as 0.1W and sense power was set as 0.2W respectively. In order to perform data transfer, Constant Bit Rate (CBR) traffic is used. Source and destination nodes for data transfer are arbitrarily chosen. The CBR traffic consists of four packets of 512 bytes/sec each.

4.2. Result

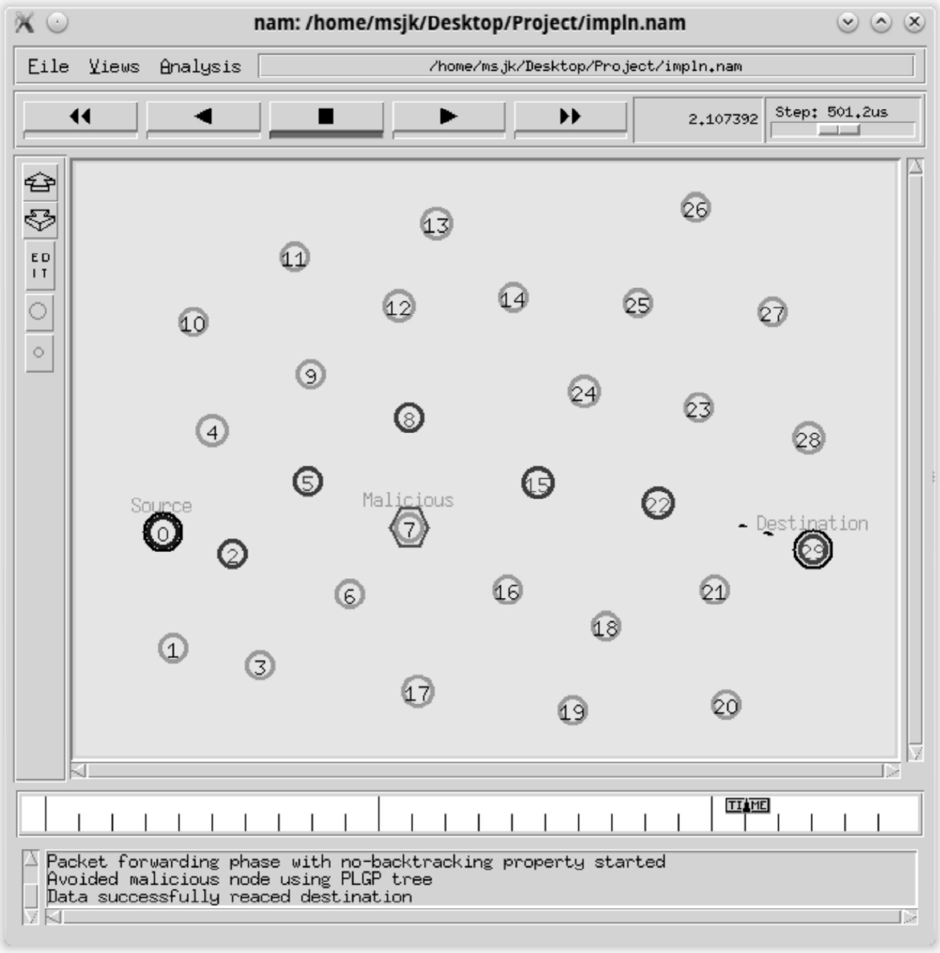
The nodes are deployed in a flat-grid topology after setting the initial positions and implementing the energy model. The routing protocol (PLGPa with modification) is associated with the topology. In Figure 5, the topology was setup with node(0) as source node, node(29) as destination and node(7) as malicious node. PLGP tree was constructed after topology discovery phase. Each node stores a copy of PLGP tree. Routing decisions are made based on this PLGP tree.

In Figure 6, the message was transmitted along with the attestation chains and signature verified by the source. When a malicious node tries to alter the route by changing the attestation chain and signature, neighbor nodes can examine the PLGP tree along with attestation chains and can detect such malicious nodes and they can re-route packets to next neighbor by avoiding that malicious node during packet forwarding phase. This increases the total hop count by one. The message reaches the destination using an alternate path which bypasses malicious node and the vampire attacks are avoided during the packet forwarding phase.



```
Topology with one malicious (node:15) and 29 honest nodes
PLGP Tree constructed after topology discovery phase
```

Figure 5: PLGP Tree construction



```
Packet forwarding phase with no-backtracking property started
Avoided malicious node using PLGP tree
Data successfully reaced destination
```

Figure 6: Message reaches destination

4.3. Result Analysis

Figure 7 shows the energy level graph. This graph shows the residual energy in nodes after message delivery from source to destination in a 30-node topology with one malicious node and 29 honest nodes. X-axis shows the time in seconds and Y-axis shows the residual energy in Joules. The existing system was prone to vampire attacks such as carousel and stretch attacks and this result in consuming more time for message delivery and reducing residual energy of nodes after message delivery. The newly implemented PLGPa with modification protocol resists vampire attacks and takes less time for message delivery and has more residual energy in nodes after message delivery.

Figure 8 shows the energy consumption graph. This graph shows the energy consumption in nodes after message delivery from source to destination. X-axis shows the time (in seconds) taken to complete the message transfer and Y-axis shows the consumed energy in joules.

Energy Consumed = Initial Energy – Minimum Residual energy among the nodes after message transfer. The existing system uses PLGP protocol and was prone to vampire attacks such as carousel and stretch attacks and this result in consuming more time for message delivery and energy of nodes for message delivery. In the graph given in figure 5, carousel attack scenario has the maximum time of 7.4 seconds to complete message transfer and maximum energy consumption of 3.917 joules. In stretch attack scenario, it takes 4.4s and 1.952J to complete message delivery. Our proposed system which uses the PLGPa with modification protocol resists vampire attacks and takes less time and energy for message delivery. The proposed system takes 2.5s and 1.389J to complete the message delivery. However, the existing system consumes less energy compared to the proposed system, when the network consists of only honest nodes.

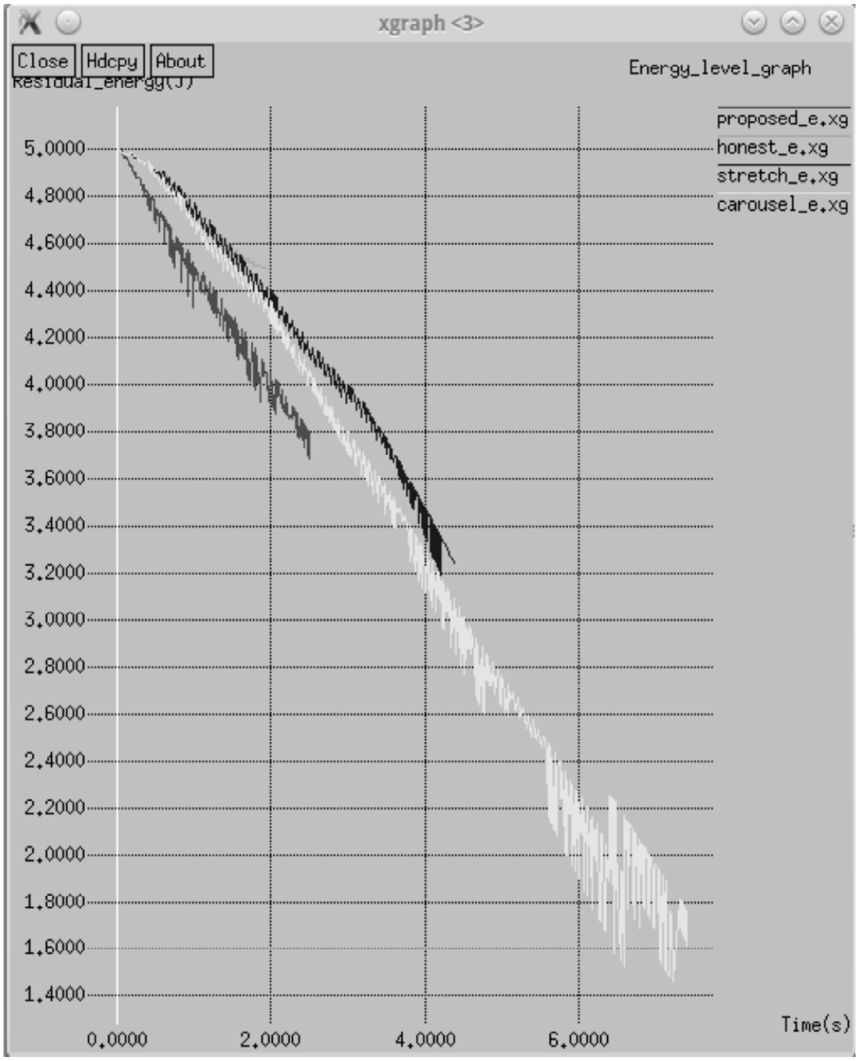


Figure 7: Energy Level Graph

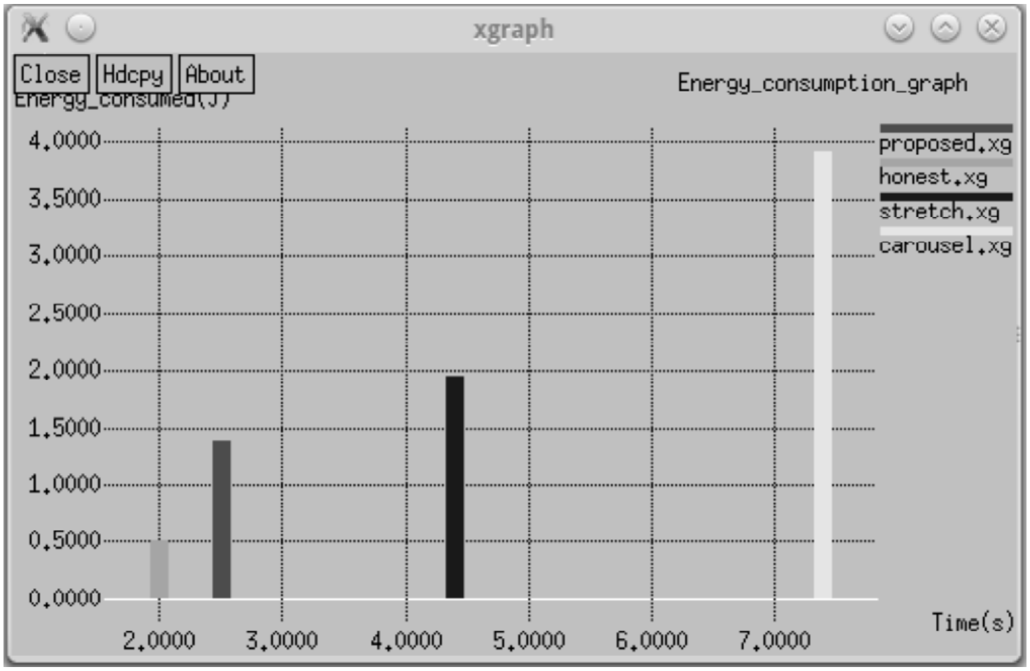


Figure 8: Energy Consumption Graph

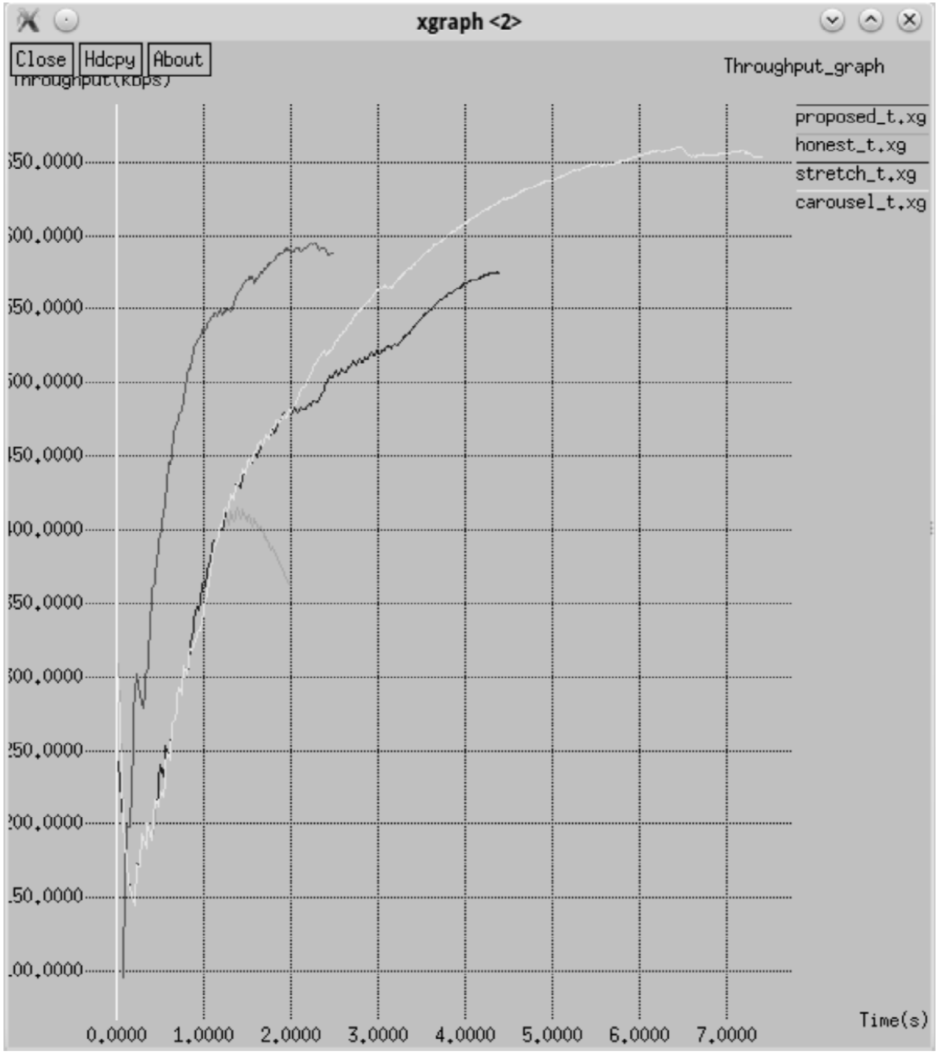


Figure 9: Throughput Graph

In the honest scenario, existing system takes 1.99s and 0.512J to complete the message transfer. Our proposed system takes slightly higher energy consumption due to the usage of additional bandwidth for attestation chains and the additional computational overhead for creating and handling them.

Figure 9 shows the throughput graph. X-axis shows the time in seconds and Y-axis shows the throughput in kilobits per second (kbps). Throughput of our proposed is substantially higher (594.94 kbps) during the entire time of its execution. We can see that, the throughput of system during carousel attack is highest (658.94 kbps) when the packet traverses through loop and the residual energy of nodes reaches critical level. The throughput is highest when the packet reaches destination, after implementing carousel attack. In the honest scenario which uses the existing PLGP protocol, throughput is lowest (408.83 kbps) because of the lesser number of packets transferred throughout the network due to the absence of vampire node. Also, the existing PLGP protocol does not incur bandwidth penalty in terms of attestation chains. However, the impact of preserving attestation chains is negligible when the damages caused by malicious nodes in various vampire attack scenarios.

5. CONCLUSION

Vampire attacks are special classes of resource depletion attacks, whose prime focus is to deplete the battery power of nodes in order to disable the network permanently. Various kinds of vampire attacks are analyzed using a 30-node topology. The network energy expenditure was found to be increasing from 50 to

100 percent depending on the location of the adversary. PLGPa with modification is a routing protocol which is made in order to reduce vampire attacks. It bounds damage from vampire attacks by verifying that the packets will make progress consistently towards their destinations. PLGPa with modification protocol has two phases–Topology Discovery phase and Packet Forwarding phase. The protocol will defend against vampire attacks at packet forwarding phase and at topology discovery phase.

References

[1] Aleksandar Kuzmanovic and Edward W. Knightly, "Low-rate TCP targeted denial of service attacks: the shrew vs. the mice and elephants," SIGCOMM, 2003.

[2] Anthony D. Wood and John A. Stankovic, "Denial of service in sensor networks," Computer 35 (2002), no. 10.

[3] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, "Secure sensor network routing: A clean-slate approach," CoNEXT, 2006.

[4] Chris Karlof and David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," IEEE international workshop on sensor network protocols and applications, 2003.

[5] Daniel J. Bernstein, Syn cookies, 1996 http://cr.yp.to/syncookies.html

[6] 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," IEEE Transactions on Vehicular Technology 58 (2009), no. 1.

[7] David R. Raymond and Scott F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," IEEE Pervasive Computing (2008), no. 1.

[8] Eugene Y. Vasserman and Nicholas Hopper, "Vampire attacks: Draining life from wireless ad-hoc sensor networks," IEEE Transactions on Mobile Computing (Volume: 12, Issue: 2), 2013.

[9] Frank Stajano and Ross Anderson, "The resurrecting duckling: security issues for ad-hoc wireless networks," International workshop on security protocols, 1999.

[10] Guang Yang, M. Gerla, and M.Y. Sanadidi, "Defense against low-rate TCP-targeted denial-of-service attacks," ISCC, 2004.

[11] Haibin Sun, John C. S. Lui, and David K. Y. Yau, "Defending against low-rate TCP attacks: dynamic detection and protection," ICNP, 2004.

[12] Haowen Chan and Adrian Perrig, "Security and privacy in sensor networks", Computer 36 (2003), no. 10.

[13] Hill J.L. and Culler D.E., "Mica: a wireless platform for deeply embedded networks," IEEE Micro 22 (2002), no. 6.

[14] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, "Denial of service resilience in ad hoc networks," MobiCom, 2004.

[15] Jae-Hwan Chang and Leandros Tassiulas, "Maximum lifetime routing in wireless sensor networks," IEEE/ACM Transactions on Networking 12 (2004), no. 4.

[16] Jing Deng, Richard Han, and Shivakant Mishra, "Defending against path-based DoS attacks in wireless sensor networks," ACM workshop on security of ad hoc and sensor networks, 2005.

[17] Jing Deng, Richard Han and Shivakant Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," Computer Communications 29 (2006), no. 2.

[18] 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.

[19] Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford, "CAPTCHA: Using hard AI problems for security," Eurocrypt, 2003.

[20] Manel Guerrero Zapata and N. Asokan, "Securing ad hoc routing protocols," WiSE, 2002.

[21] Mina Guirguis, Azer Bestavros, Ibrahim Matta, and Yuting Zhang, "Reduction of quality (RoQ) attacks on Internet end-systems," INFOCOM, 2005.

[22] Padmavathi. G, Shanmugapriya. D,"A Survey of Attacks, Security Mechanisms and challenges in Wireless Sensor Networks,"International Journal of Computer Science and Information Security, IJCSIS 2009.

[23] Savitha. M, Manavalan. R "Efficient Data Transmission Using Energy Efficient Clustering Scheme for Wireless AdHoc Sensor Network" International Journal of Computer Trends and Technology (IJCTT)–volume 17 number 2–Nov 2014.

[24] Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak, and Jennifer Rexford, "Path-quality monitoring in the presence of adversaries," SIGMETRICS, 2008.

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

[26] Subhashini.S.J., Nagalakshmi. K, Kumudha. M, Rincy. K.R,” Enduring and Securing Network Node’s Life using PLGP”, International Journal of Scientific Engineering and Applied Science (IJSEAS)-Volume-1, Issue-4, July 2015

[27] Timothy J. McNevin, Jung-Min Park, and Randolph Marchany, “pTCP: A client puzzle protocol for defending against resource exhaustion denial of service attacks,” Technical Report TR-ECE-04-10, Department of Electrical and Computer Engineering, Virginia Tech, 2004.

[28] Tuomas Aura, ‘Dos-resistant authentication with client puzzles, International workshop on security protocols,’ 2001.

[29] Xiapu Luo and Rocky K. C. Chang, “On a new class of pulsing denial-of-service attacks and the defense,” NDSS, 2005.

[30] 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.

[31] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, “Ariadne: A secure on-demand routing protocol for ad hoc networks,” MobiCom, 2002.

[32] Yu-Kwong Kwok, Rohit Tripathi, Yu Chen, and Kai Hwang, “HAWK: Halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks,” Networking and mobile computing, 2005.