ijecs
open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 03 Issue 07 July, 2014 Page No. 6888-6895

A light weight PLGP based method for mitigating vampire attacks in Wireless Sensor Networks

Farzana T[1], Mrs.Aswathy Babu [2]

[1]MTech in computer science and engineering,
MES Engineering College, Kuttippuram, Kerala
farsanat@gmail.com

[2]Asst.Prof in Computer science and engineering,
MES Engineering College, Kuttippuram, Kerala
aswathymes@gmail.com

,

Abstract: ***Deployment of sensor network in hostile environment makes it mainly vulnerable to battery drainage attacks because it is impossible to recharge or replace the battery power of sensor nodes. The motivation of a large portion of research efforts has been to maximize the network lifetime, where the lifetime of network is measured from the instant of deployment to the point when one of the nodes has exhausted its limited power source and becomes in-operational commonly referred as first node failure. But there is a class of resource consumption attack called vampire attack which permanently disables the whole network by quickly draining nodes battery. In this novel approach, forwarding as well as discovery phase of the protocol are considered to avoid attack. Here algorithm overhead is reduced and discovery phase is considered to avoid vampire attack.***

Keywords: Wireless Sensor Network, Denial of Service, multi-path routing, opportunistic routing, energy efficiency

I. INTRODUCTION

Wireless Sensor Networks WSN is a collection of wireless nodes with limited energy capabilities that may be mobile or stationary and are located randomly on a dynamically changing environment. The routing strategies selection is an important issue for the efficient delivery of the packets to their destination. Moreover, in such networks, the applied routing strategy should ensure the minimum of the energy consumption and hence maximization of the lifetime of the network. One of the first WSNs was designed and developed in the middle of the 70s by the military and defence industries. WSNs were also used during the Vietnam War in order to support the detection of enemies in remote jungle areas. However, their implementation had several drawbacks. It includes the large size of the sensors, the energy they consume and the limited network capability. Since then, a lot of work on the WSNs field has been carried out resulting in the development of the WSNs on a wide variety of applications and systems with vastly varying requirements and characteristics. At the same time, various energy-efficient routing protocols have been designed and developed for WSNs in order to support efficient data delivery to their destination. Thus, each energy-efficient routing protocol may have specific characteristics depending on the application and network architecture. The WSNs may be used in a variety of everyday life activities or services. For example a common application of WSNs is for monitoring. In the area of monitoring, the waves, different types of wireless communicating devices and also equipped with an energy source such as battery. The entire network works simultaneously by using sensors of different dimensions and a routing algorithm. They are mainly focused on providing delivery data from the source to the destination nodes.

WSN is deployed over a region in order to monitor some phenomenon. A practical use of such a network could be a military use of sensors to detect enemy intrusion.

1.1 Energy consumption and Network lifetime of WSN

1.1.1 Energy consumption in WSN

The research and development of routing protocols in WSNs were initially driven by defence applications. Sensor networks consist of a small or large amount of nodes called sensor nodes. These nodes are varying in size. Based on this, the sensor nodes work efficiently in different fields. WSNs have such sensor nodes which are specially designed in such a typical way that they include a micro-controller which controls the monitoring, a radio transceiver for generating radio

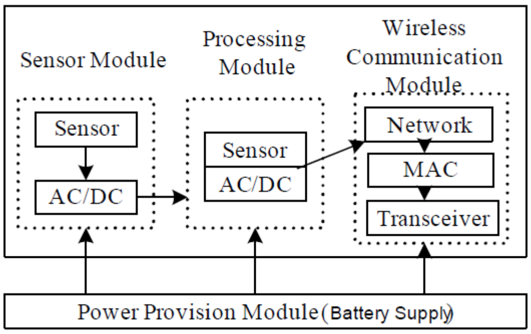


Figure 1.1: WSN node architecture

The WSN nodes consist of several modules as shown in figure. They are Sensor Module, Processing Module, Wireless Communication Module and Power Supply Module. These components work together in order to make the sensor operational in a WSN environment.

1.1.2 Network Lifetime

In many cases the term network lifetime corresponds to the time when the first node exhausts its energy, or when a certain fraction of the networks nodes is dead, or even when all nodes are dead. In some other cases it may be reasonable to measure the network lifetime by application-specific parameters, such as the time when the network can no longer relay the video. The importance of a WSN is to be operational and able to perform its tasks during its use. In WSNs, it is important to maximize the network lifetime, which means to increase the network survivability or to prolong the battery lifetime of nodes.

2. Related Works

Most of the research on this topic is revolved around security solutions using the layered approach. In layered approach the protocol stacks consists of the physical layer, data link layer, network layer, transport layer and application layer. These five layers and the three planes, i.e., the power management plane, mobility management plane and task management plane jointly forms the wireless layered architecture. Researchers are always being conducted to improve the energy efficiency of the wireless Sensor Networks. Some of the approaches are described. They are

i. Wireless Sensor Network Denial of Sleep attack[1]
ii. Intrusion Tolerant routing in Wireless Sensor Network[2]
iii. Cross-Layer Design for Energy Conservation in Wireless Sensor Network[3]
iv. Energy Efficient Opportunistic Routing in Wireless Sensor Network[4]
v. Optimal sleep-wake scheduling for quickest intrusion detection using sensor networks[10]
vi. Sleep Deprivation Attack Detection in Wireless Sensor Network[5]
vii. Vampire Attack: Draining Life from Wireless Sensor Network[6]

2.1 Denial of sleep attack

Michael Brownfield[1] discussed the energy resource vulnerabilities at MAC level. Denying sleep effectively attacks each sensor node's critical energy resources and rapidly drains the network's lifetime so proposed a new G-MAC protocol to control the sleep awake pattern of sensor nodes. G-MAC has several energy saving features which not only show promise in extending the network lifetime, but the centralized architecture makes the network more resistant to denial of sleep attacks. This scheme performs well in all traffic situations but deals only with MAC layer depletion attack

2.2 Intrusion tolerant routing

The Jing Deng, Richard Han, Shivakanth mishra[2] proposed an Intrusion tolerant routing protocol for WSN. INSENS constructs a forwarding table at each node to facilitate communication between sensor nodes and base station. In INSENS each node shares a secret key only with the base station and not with any other nodes. This has advantage in case a node is compromised that an intruder will only have access to one secret keys rather than the secret keys of neighbors and other nodes throughout the network. It also provides multi path routing and minimize the communication, storage and computation requirements of sensor node at the expense of increased requirements at base station.

2.3 Cross layer approach

Fatma Bouabdullah, Nizar Bouabdullah, Raouf Bouabdullah [3] proposed a cross layer strategy that considers routing and MAC layers jointly. A network lifetime is time for the first node in wireless sensor network to fail. An efficient routing protocol would drain energy slowly and uniformly among nodes leading to the death of all nodes nearly at same time. At routing level they proposed that sending data through multiple paths instead of using a single path so can balancing energy consumption. At MAC level limits the retransmission over each wireless links according to its property and the required packet delivery probability, but this scheme does not considers any attack.

2.4 Opportunistic routing method

Xufei Mao,Shaojie Tang, Xiahua Xu & Huadong Ma[4] focused on opportunistic method to minimize energy consumption by all nodes but this method does not consider any attack at routing level. Opportunistic routing is based on the use of broadcast transmission to expand the potential forwarders that can assist in the retransmission of data packets. By this method nodes in the forwarder list are prioritized and the lower priority forwarder will discard the packet if the packet has been forwarded by a higher priority forwarder.

2.5 Optimal sleep-wake scheduling for intrusion detection

K.Premkumar and Anurag Kumar[10] proposed a protocol that uses markov decision process models to identify the malicious nodes quickly with the use of minimal set of sensor nodes in active state. By using a minimal number of sensor devices, it ensures that the energy expenditure for sensing , computation and communication is minimized and so the lifetime of network is maximized.

2.6 Sleep deprivation attack

Tapaliana Bhattasali[5] proposed an frame work based on distributive collaborative mechanism for detecting sleep deprivation attack increased energy efficiency but does not considers routing layer.Sleep deprivation torture comes in the form of sending useless control traffic and forces the node to forgo their sleep cycles so that they are completely exhausted and hence stop working.Here workload is distributed among components according to their capacity to avoid complete exhaustion of battery power. Packet transmission overhead may high in some cases and its main advantage is it enhances energy efficiency and network scalability.

3. **VAMPIRE ATTACKS: DRAINING LIFE FROM WIRELESS SENSOR NETWORKS**

Vampire attack [6] is an instance of denial of service attack and it can be defined as the composition and transmission of a message that causes more energy to be consumed by the network than if a honest node transmitted a message of identical size to the same destination, although using different packet headers. The strength of the attack can be measured by the ratio of network energy used in the benign case to the energy used in the malicious case, i.e., the ratio of network-wide power utilization with malicious nodes present to energy usage with only honest nodes when the number and size of packets sent remains constant. Safety from Vampire attacks implies that this ratio is 1. Energy used by malicious nodes is not considered since they can always unilaterally drain their own batteries.

These attacks do not disrupt immediate availability, but rather work over time to entirely disable a network. This type of attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes. Neither do these attacks rely on flooding the network with large amounts of data, but try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent.

3.1 Directional antenna attack

Main cause of vampire attack is directional antenna attack. Vampires have little control over packet progress when forwarding decisions are made independently by each node, but they can still waste energy by restarting a packet in various parts of the network. Using a directional antenna adversaries can deposit a packet in arbitrary parts of the network, while also forwarding the packet locally.

This attack can be considered a half-wormhole attack, since a directional antenna constitutes a private communication channel, but the node on the other end is not necessarily malicious. It can be performed more than once, depositing the packet at various distant points in the network, at the additional cost to the adversary for each use of the directional antenna. There are two types of vampire attacks based on this directional antenna attack. They are Stretch attack and carousel attack.

carousel attack: In carousel attack, an adversary composes packets with purposely introduced routing loops. It sends packets in circles as shown in Fig 3.1. It targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes.

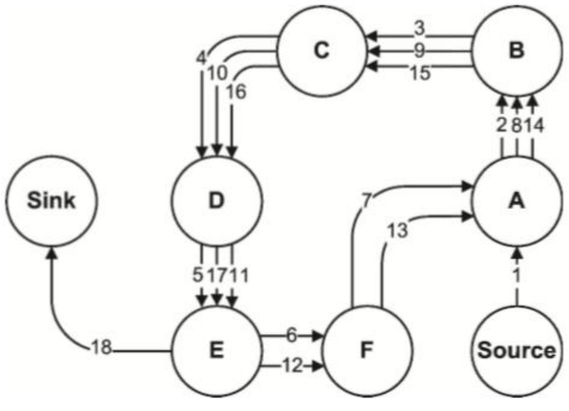


fig 3.1 carousal attack

Stretch attack: In Stretch attack, an adversary constructs artificially long routes, potentially traversing every node in the network. It increases packet path lengths, causingpackets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination. An example is illustrated in Fig 3.2.

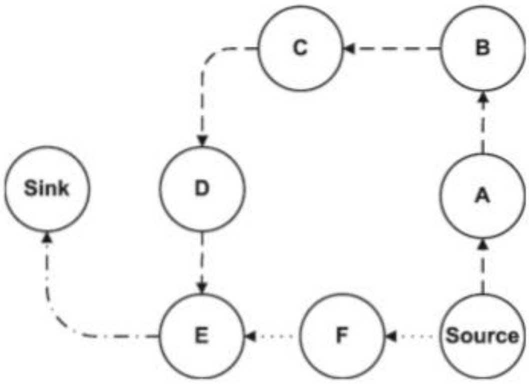


fig 3.2 Stretch attack.

In a randomly generated topology, a single attacker can use a carousel attack to increase energy consumption by as much as a factor of 4, while stretch attacks increase energy usage up to an order of magnitude, depending on the position of the malicious node. The impact of these attacks can be further increased by combining them, increasing the number of adversarial nodes in the network, or simply sending more packets. Although in networks that do not employ authentication or use end-to-end authentication, adversaries are free to replace routes in any overheard packets and assume that only messages originated by adversaries may have maliciously composed routes.

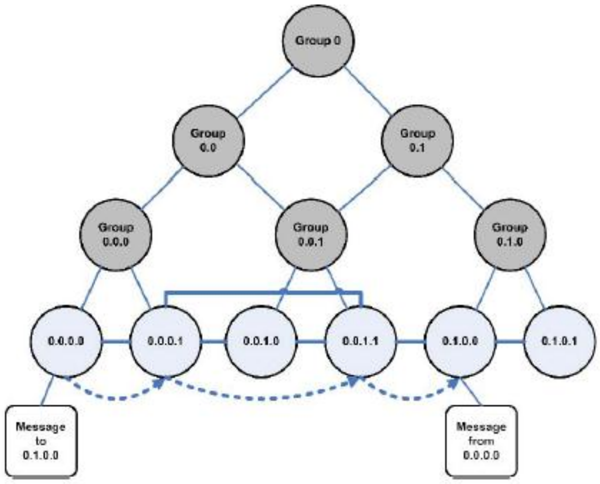
3.2 Clean-state sensor network routing

A clean-state secure sensor network routing protocol is an efficient, highly resilient to active attacks. This protocol[8] is introduced by Bryan Parno, Mark Luk, Evan Gaustad, Adrian Perrig(PLGP from here on). It has two phases, they are topology discovery phase and packet forwarding phase. The original version of the protocol, although designed for security, is vulnerable to Vampire attacks. Here PLGP can be modified to provably resist. Vampire attacks during the packet forwarding phase.

Topology discovery : Discovery deterministically organizes nodes into a tree that will later be used as an addressing scheme. When discovery begins, each node has a limited view of the network, the node knows only itself. Nodes discover their neighbours using local broadcast, and form ever expanding neighbourhoods, stopping when the entire network is a single group. Throughout this process, nodes build a tree of neighbour relationships and group membership that will later be used for addressing and routing. Discovery begins with a time limited period during which every node must announce its presence by broadcasting a certificate of identity, including its public key, signed by a trusted offline authority. Each node starts as its own group of size one, with a virtual address 0. Nodes who overhear the presence broadcasts form groups with their neighbours. When two individual nodes (each with an initial address 0) form a group of size two, one of them takes the address 0, and the other becomes 1. Groups merge preferentially with the smallest neighbouring group, which may be a single node. Like individual nodes, each group will initially choose a group address 0, and will choose 0 or 1 when merging with another group. Each group member prepends the group address to their own address, node 0 in group 0 becomes 0.0, node 0 in group 1 becomes 1.0, and so on. Each time two groups merge, the address of each node is lengthened by 1 bit. Implicitly, this forms a binary tree of all addresses in the network, with node addresses as leaved. Note that this tree is not a virtual coordinate system, as the only information coded by the tree are neighbour relationships among nodes.

When larger groups merge, they both broadcast their group IDs (and the IDs of all group members) to each other, and proceed with a merge protocol identical to the two node case. Groups that have grown large enough, some members are not within radio range of other groups will communicate through gateway nodes, which are within range of both groups. Each node stores the identity of one or more nodes through which it
hear an announcement that another group exists. Since every group members knows the identities of all other group members and the network converges to a single group, each node learns every other node's virtual address, public key, and certificate at the end of discovery phase

Packet forwarding: During the forwarding phase, all decisions are made independently by each node. When receiving a packet, a node determines the next hop by finding the most significant bit of its address that differs from the message originators address as shown in figure. Leaves represent physical nodes, connected with solid lines if within radio range. The dashed line is the progress of a message through the network. Note that nonleaf nodes are not physical nodes but rather logical group identifiers. Thus every forwarding event (except when a packet is moving within a group in order to reach a gateway node to proceed to the next group) shortens the logical distance to the destination, since node addresses should be strictly closer to the destination.



Following function *forward_packet* defines the packet forwarding process in PLGP

```
Algorithm 1 Forward_packet(p)
  $s \leftarrow extract\_source\_address(p)$
  $c \leftarrow closest\_next\_node(s)$
  if (is_neighbour(c)) then
    forward(p,c)
  else
    $r \leftarrow next\_hop\_to\_non\_neighbour(c)$
    forward(p,r)
  end if
```

In PLGP, forwarding nodes do not know what path a packet took, allowing adversaries to divert packets to any part of the network, even if that area is logically further away from the destination than the malicious node. This makes PLGP vulnerable to Vampire attacks. So forwarding phase of PLGP is modified to avoid vampire attacks. No-backtracking property, is satisfied for a given packet if and only if it consistently makes progress toward its destination in the logical network address space. To preserve no-backtracking, we add a verifiable path history to every PLGP packet. The resulting protocol, PLGP with attestations (PLGPa) uses this packet history together with PLGPs tree routing structure so every node can securely verify progress, preventing any significant adversarial influence on the path taken by any packet which traverses at least one honest node. Whenever node n forwards packet p, it this by attaching a non replayable attestation (signature). These signatures form a chain attached to every packet, allowing any node receiving it to validate its path. Every forwarding node verifies the attestation chain to ensure that the packet has never travelled away from its destination in the logical address space. Following function *Secure _forward _packet(p)* defines the modified protocol.

```
Algorithm 2 Secure_ forward_packet(p)
  $s \leftarrow extract\_source\_address(p)$
  $a \leftarrow extract\_attestation(p)$
  if (not verify_source_sig(p)) or (empty(a) and not is_neighbour(s)) or (not
  saowf_verify(a)) then
    return /*drop(p)*/
    for all node in a do
      $prevnode \leftarrow node$
      if (not are_neighbours(node,prevnode)) or (not making_progress(prevnode,node))
      then
        return /*drop(p)*/
      end if
    end for
  end if
  $c \leftarrow closest\_next\_node(s)$
  $P \leftarrow saowf\_append(p)$
  if (is_neighbours(c)) then
    forward(P,c)
  else
    forward(P,next_hop_to_non_neighbour(c))
  end if
```

4. PROBLEM DEFINITION

The vampire attack is a serious problem in wireless sensor networks. Such attacks need to be detected as early as possible. PLGPa is the protocol that bounds damage from vampire attack, but this has several drawbacks. They are defined below PLGPa includes path attestations, increasing the size of every packet, incurring penalties in terms of bandwidth use, and thus radio power. Adding extra packet verification requirements for intermediate nodes also increases processor utilization, requiring time, and additional power.

Energy expenditure for cryptographic operations at intermediate hops is, much greater than transmit or receive overhead, and much more dependent on the specific chipset used to construct the sensor. While PLGPa is not vulnerable to Vampire attacks during the forwarding phase, but it does not offer a satisfactory solution during the topology discovery phase.

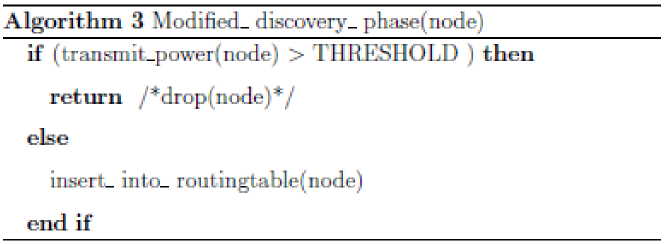
5. LIGHT WEIGHT PLGP BASED METHOD TO AVOID VAMPIRE ATTACK

The proposed work provides solution for the two problems in the existing method.

5.1 Implementation

In the proposed work, light weight PLGP based method, mainly focused on avoiding vampire attacks in the discovery phase of PLGP by checking signal strength of the nodes which transmit the group joining messages. A vampire would send high energy signal so as to suppress the group joining messages of other node. So avoid a node which sends at high signal strength.

Following function modified discovery phase(node) defines this concept.



```
Algorithm 3 Modified_ discovery_ phase(node)
  if (transmit_power(node) > THRESHOLD ) then
    return  /*drop(node)*/
  else
    insert_ into_ routingtable(node)
  end if
```

Another focus is to reduce overhead of PLGPa by using single encryption instead of chain of encryption.

Existing method concept

A =) B =) C =) D =) E
If A wants to sent any information to E through B,C,D then attestation process includes following steps:

- Encrypt the message using a secret key, then the packet includes encrypted data,cost of the operation, sender's identity (A). The whole data are encrypted with private key of A then this packet send to B.

  ENC((Msg)Prk,4,A)PrA== X =) B
- When B receives this packet, B adds the cost and its path information to the packet. This entire packets sends to C

  B =) DEC(X)PA =) ENC(X,3,AB)PrB == Y =) C
- When C receives the packet, above process will repeat as shown below:

  C =) DEC(Y)PB =)ENC(Y,2,ABC)PrC == Z =) D
  D =) DEC(Z)PC =)ENC(Z,1,ABCD)PrD =) E

Proposed method concept

In this novel method the attestation process is as shown below:

- Encrypt the message using a secret key, then the packet includes encrypted data, cost of the operation, sender's identity (A). The whole data are encrypted with private key of A then this packet send to B as in previous case.

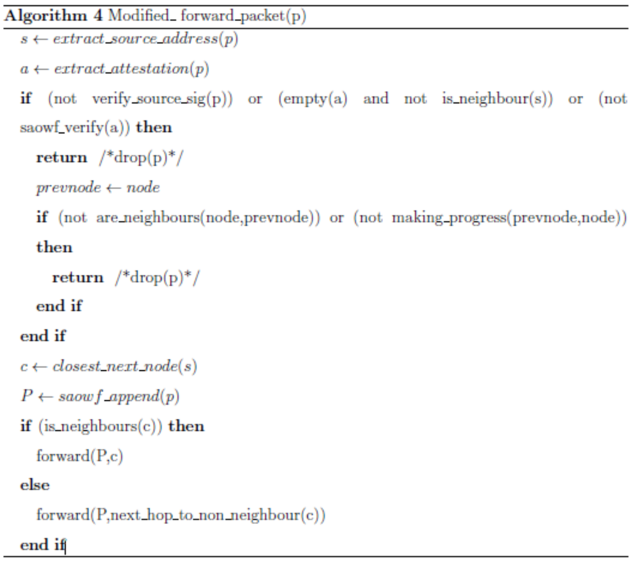
  ENC((Msg)Prk,4,A)PrA == X =) B
- When B receives the packet decrypts it and retrieves the encrypted message only. After retrieving the encrypted message B then includes the path information along with the updated cost into the packet. These whole informations are encrypted with B's private key and send to C.

B =) DEC(X)PA =) ENC((Msg)Prk,3,AB)PrB == Y =) C

- When C receives the packet, above process will repeat as shown below:

C =) DEC(Y)PB =)ENC((Msg)Prk,2,ABC)PrC == Z =) D
D =) DEC(Z)PC =)ENC((Msg)Prk,1,ABCD)PrD =) D

Based on these concepts *Secure_forward_packet(p)* can be modified as shown below:



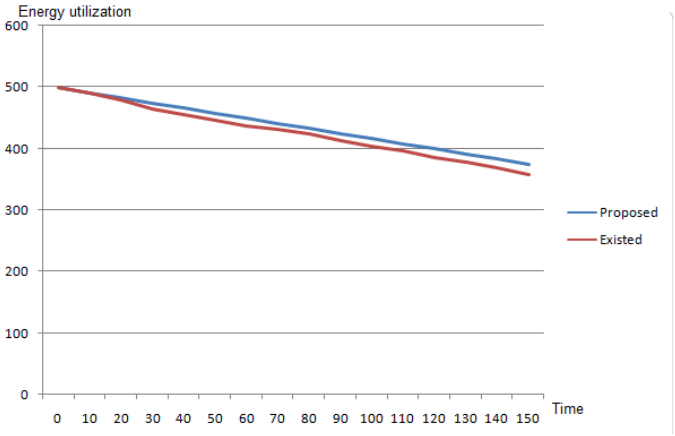
```
Algorithm 4 Modified_ forward_packet(p)
  s ← extract_source_address(p)
  a ← extract_attestation(p)
  if (not verify_source_sig(p)) or (empty(a) and not is_neighbour(s)) or (not
  saowf_verify(a)) then
    return  /*drop(p)*/
    prevnode ← node
    if (not are_neighbours(node,prevnode)) or (not making_progress(prevnode,node))
    then
      return  /*drop(p)*/
    end if
  end if
  c ← closest_next_node(s)
  P ← saowf_append(p)
  if (is_neighbours(c)) then
    forward(P,c)
  else
    forward(P,next_hop_to_non_neighbour(c))
  end if
```

6. EXPERIMENTAL RESULTS

Vampire attacks possess a serious threat to security of wireless sensor network. The proposed work has been compared based on various parameters. The various parameters used are energy utilization, packet overhead, number of packet drops, encryption overhead, time spent for encryption etc.

Every node's initial energy is set as 500 joules. Energy utilization of a node in existing and proposed methods are shown in Figure 6.3

Figure 6.3: Energy utilization Vs Time



Number of packet drops of the proposed system and existing method is shown in Figure 6.4. Here vampire attacks are identified in discovery phase also. So chances of composition and transmission of unwanted data packets are reduced, if a node is identified as vampire node. Hence in figure 6.4 packet drop rate is higher than the existing method. Packet overhead of the proposed system and existing method is shown in figure 6.5.

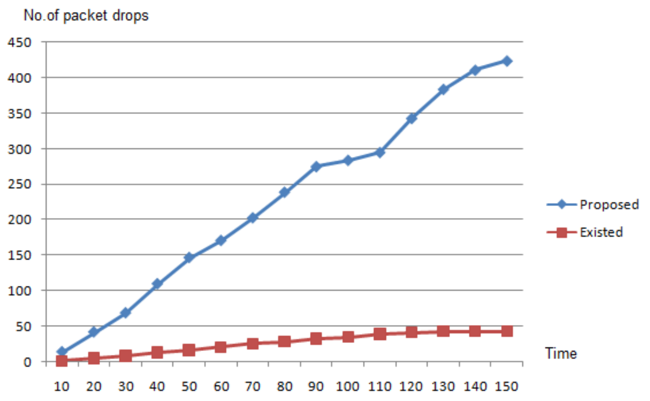


fig 6.4 Number of packet drops Vs Time

Because of the chain attestation process size of the packet in existing method is higher than proposed method. From the figure it is clear that the packet size is reduced here.

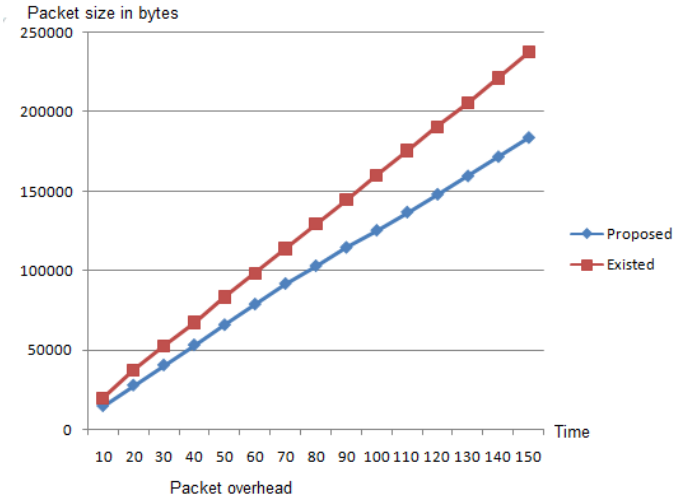


fig 6.5 Packet size Vs Time

Number of encryptions of the proposed system and existing method is shown in Figure 6.6. From the figure it is clear that the encryption overhead is reduced by reducing the chain attestation process. Since the number of encryptions of the proposed system is reduced in figure 6.6, following figure shows the time taken for the encryption process in proposed and existing method. From the figure it is clear that the time taken to attest a packet is reduced.

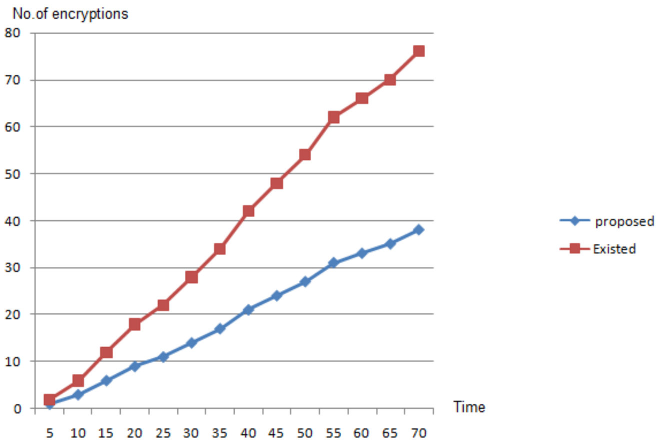


fig 6.6 No.of encryptions Vs Time

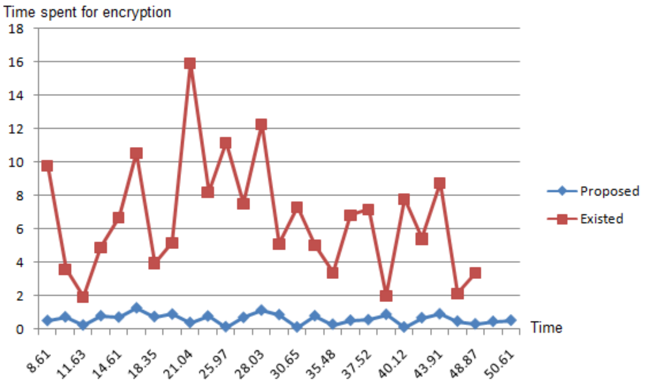


fig 6.7 Time spent for encryption Vs Time

7.CONCLUSION AND FUTURE WORKS

The Wireless Sensor Network is an emerging area which has wide applications. Hence the security in wireless sensor network is of great concern. Vampire attacks are important attack against a wireless sensor network in which an adversary develop and transmit messages that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers. So it is very important to detect the vampire nodes as early as possible.

Here PLGP protocol is used to employ the vampire attacks. Since PLGP has two phases vampire node detection is also done in this two phases. The novel algorithm is the first sensor network routing protocol that provably bounds the damage from vampire attack in two phases of PLGP. This method reduces the energy utilisation, packet overhead, encryption efforts etc. Here only PLGP protocol is considered, how the proposed solution works in other routing protocol is not considered. This method can be further extended to determine this problem.

REFERENCES

[1] Michael Brownfield,Yatharth Gupta, ”Wireless Sensor Network Denial of Sleep Attack”, Proceedings of 2005 IEEE workshop on information assurance,June 2005.

[2] Jing Deng, Richard Han, Shivakanth mishra, ”INSENS: IntrusionTolerant routing in Wireless Sensor Networks”, University of Colorado, Department of computer science Technical report,June 2006 .

[3] Fatma Bouabdullah, Nizar Bouabdullah,Raouf Bouabdullah ”Cross-layer Design for Energy Conservation in Wireless Sensor Networks”, IEEE GLOBECOM 2008,New Orleans,USA,December 2008.

[4] Xufei Mao,Shaojie Tang, Xiahua Xu, ”Energy efficient Oppurtunistic Routing in Wireless Sensor Networks”, IEEE transactions on parellel and distributed systems, VOL. 12, NO. 2, February 2011

[5] Tapaliana Bhattasali,Rituparna Chaki,Sugata Sanyal ”Sleep Deprivation Attack Detection in Wireless Sensor Networks”, International journal of computer applications(0975-8887)vol 40- No: 15,February 2012

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

[7] Yazeed Al-Obaisat,Robin Braun, ”On Wireless Sensor Networks: Architectures, Protocols,Applications and Management”, Institute of Information and Communication Technologies,May 2004

[8] B.Prano, M.Luk, E.Gustad, A.Perrig, ”Secur Sensor Network Routing: A Clean-state Approach”, CoNEXT:Proc.ACM CoNEXT Conf.,2006

[9] D.B. Johnson, D.A Maltz, J.Broch, ”DSR: The Dynamic Source Routing Protocol for Multihop Wireless Adhoc Networks”, Adhoc Networking, Addison Wesley, 2001

[10] K.Premkumar and Anurag Kumar, ”Optimal sleep-wake scheduling for quickest intrusion detection using sensor networks ”, IEEE explore, February, 2008

Author Profile

Farzana T received the bachelor’s degree in Computer science and engineering from the Calicut University, Kerala in 2008. Presently she is pursuing her M.Tech in the department of Computer Science and Engineering from Calicut University, Kerala. She has teaching experience of three and half years. Her research interests include wireless sensor networks, cryptography and network security, wireless security etc.