Vampire Attack Prevention to reduce Node Power Consumption in WSN

Laxmi Choukiker
M.tech scholar
Department of CSE
Truba institute of engineering&
information technology, Bhopal

Amit Saxena
Associate Professor
Department of CSE
Truba institute of engineering&
information technology, Bhopal

Manish Manoria, PhD
Professor
Department of CSE
Truba institute of engineering&
information technology, Bhopal

ABSTRACT

Mobile unintended network (WSN) area unit self-configuring, individual nodes or routers networks that move concerning freely, organize themselves randomly and area unit reticulated through wireless links that once synchronized, type a dynamic topology. The attackers during this reasonably network area unit simply changed the first routing performance by that the unfinished energy resource of nodes area unit wasted. The nodes in needed battery power for communication and it's terribly crucial concern operate the battery power of nodes with efficiency in network with none interference of aggressor. during this analysis we tend to projected a brand new energy economical routing theme with AODV routing protocol against evil spirit attack to enhance the consistency of information delivery and energy utilization. The projected IPS (Intrusion detection and hindrance System) routing theme is utilizing the energy of mobile nodes. The evil spirit aggressor is flooded the massive range of packets in network due to that ordinary intermediate nodes area unit received that packets and their energy is wasted for receiving these unwanted packets. The projected IPS is known the aggressor by their gratuitous energy consumption of mobile nodes. The network performance in presence of IPS is provides secure routing as adequate traditional routing performance. The evil spirit aggressor information loss existence in presence of IPS is marked zero e.g. the sign of reliable and secures routing. The routing performance is measured through performance matrices and therefore the projected methodology is showing the far better performance as compare to aggressor presence in network.

Keywords

Energy, Vampire attack, WSN, AODV, routing, performance.

1. INTRODUCTION

Wireless sensing element Network (WSN) is Associate in Nursing autonomous system of mobile nodes connected by wireless links; every node operates as Associate in Nursing finish system and a router for all alternative nodes within the network [1]. WSN network may be a cluster of wireless mobile computers (or nodes); during which nodes collaborate by forwarding packets for every alternative to permit them to speak outside vary of direct wireless transmission. sensing element networks need no centralized administration or fastened network infrastructure like base stations or access points, and might be quickly and inexpensively came upon pro re nata. this implies that 2 nodes cannot communicate with one another once the gap between the 2 nodes is on the far side the communication vary of their own. WSN solves this drawback by permitting intermediate parties to relay knowledge transmissions. The attackers in WSN area unit simply affected the conventional network performance thanks to absence of coordination system [2]. There are a unit two styles of attacks in network 1st is active and another one is passive. Active offenders area unit terribly harmful as a result of they are hammer and deform the full network performance however their detection and hindrance is feasible however passive attackers aren't distort complete network performance however slightly quantity of knowledge is stricken by that this sort of attacker aren't recognized simply. The attacker's classification intimately mentioned in [2].

In active attack, malicious nodes or offender nodes in network area unit liable for packets dropping because of routing wrongdoing [1]. The routing performance of network is degrades thanks to significant packet dropping. Mobile and self organizing characteristics of WSN makes a superb prospect, however, it faces plenty of security problems. for instance, key management and authentication, routing security, intrusion detection, and enhance cooperation. Intrusion detection is security technology, that finds that a network or system whether or not there's any breach of security strategy and therefore the sign of invasion that's through network or system from variety of key points within the assortment of knowledge and analysis. the numerous IDS schemes [3] known the offender wrongdoing and hinder their existence. The IDS Security theme not solely detected however conjointly forestall from offender.

These routing protocols [4, 5] in WSN area unit just like and are available as a natural extension of these for the wired networks. In proactive routing, every node has one or a lot of tables that contain the newest data of the routes to any node within the network. The reactive routing protocol is provided with another denomination named on-demand routing protocol. In compare to the proactive routing, the reactive routing is solely starts once nodes need to transmit knowledge packets. The hybrid routing protocol because the name suggests have the mix blessings of proactive routing and reactive routing to beat the defects generated from each the protocol once used individually.

Vampire Attack is that the kind of attack consumes the energy of traditional node and reduce the performance of the network and whereas node energy utilized by fuse less packet than network split in variety of sub network and increase the network overhead. The planned secure IDS is provides the offender free routing by known it through calculate the trail length hand-picked by the offender false reply. the protection system is apply the protection procedure to it wrong path and known the destination reach ability from that path. The destination make striation is additionally confirm the info isn't received then, known the malicious nodes and blocks their functioning for providing secure communication.

2. RELATED WORK

It has been observed that although active research is being carried out area of security in WSN, the proposed solutions are not complete in terms of effective and efficient routing security against malicious attack but slightly strike the idea of new research. The some previous works are discussed in this section. We can classify the attacks in to brief categories, There are some researchers are doing a work on attacks mentioned in this section.

Eugene Y. Vasserman and Nicholas Hopper [1] "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks" This title explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. We find that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol-compliant messages. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O(N), where N in the number of network nodes. We discuss methods to mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.

Ankita Shrivastava, Rakesh Verma[4] "Detection of Vampire Attack in Wireless Ad-hoc Network" in this title we describe a Vampire attacks modify targeted packets. It does so by preparing long routes or misguiding the packets. Malicious nodes use false messaging, or modify routing information. This action affects the bandwidth and node battery power. Routing as well as network resources gets protection from vampire attack; an approach is proposed to detect malicious routing packets.

Anoopa S, Sudha S K.[5] "Detection and Control of Vampire Attacks in Ad-Hoc Wireless Networks"in this title we discuss work explores the identification of resource depletion attacks at the routing protocol layer and in the application layer, which permanently disable networks by quickly draining nodes' battery power. These Vampire attacks are not specific to a particular protocol, but rather rely on the properties of many popular classes of routing protocols. It is clear that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages.

K.Vanitha,V.Dhivya [6] "A Valuable Secure Protocol to Prevent Vampire Attacks In Wireless Ad Hoc Sensor Networks" in this title we have discuss Ad hoc require no centralized administration so the network infrastructure can be formed quickly and inexpensive set up is needed. Ad hoc networks are being used in military operation, emergency disaster relief and community networking. An important security issue that has been identified in these networks is resource depletion attack at routing layer protocol. These attacks drain nodes battery power completely, so that the network is permanently disabled. Hence these attacks are termed as vampire attacks. Even as there exist many secure routing protocols, they are unable to protect the network from vampire attacks. So as an attempt to eliminate vampire attacks, three primary contributions has been introduced.

Gowthami.M, Jessy Nirmal.A.G,P.S.K.Patra [7] "Mitigating Vampire Attack in Wireless Ad-Hoc Sensor Networks" in This title a technique to tolerate the attack by employing the Cluster Head. In case of each Vampire attack, the Cluster Head employs in this situation and distributes the packet to destination without dropping the packet. Thus give a successful and reliable message delivery even in case of Vampire attack. In the worst case, a single Vampire can increase networkwide energy usage by a factor of O(N), where N is the number of network nodes.

Ambili M. A, Biju Balakrishnan,[8] "Vampire Attack: Detection and Elimination in Wsn" The title we focus on the way in which the attack can be overcome in the best possible manner. The proposed system describes some methods and alternative routing protocols solution that help to detect and eliminate vampire attack and thus make the network live.

Kirthika.K, Mr.B.Loganathan, [9] "Vampire Attacks In Wireless Sensor Network –A Survey" in this title we proposed considers a new class of resource consumption attacks which is defined and named as Vampire attacks which is not clearly defined earlier in routing protocols and also vary under stateless and state ful routing protocols . Here network routing protocol prevents data from Vampire attacks by verifying packets consistently and makes progress toward their destinations with the verification and forwarding scheme.

P.Rajipriyadharshini,V.Venkatakrishnan,S.Suganya,A.Masanam,[10] "Vampire Attacks Deploying Resources in Wireless Sensor Networks" in this title we discuss Now-a-days one main issue in wireless ad-hoc sensor network is wastage of energy at each sensor nodes. Energy is the one most important factor while considering sensor nodes. Wireless sensor networks require solution for conserving energy level. One new type of attack called vampire attack, which occurring at network layer. It leads to resource depletion (energy) at each sensor nodes, by destroying battery power of any node. It transmit a small complaint messages to disable a whole network, hence it is very difficult to detect and prevent. Existing protocols are not focusing on this vampire attack happening on routing layer, hence there exist two types of attacks namely, carosuel and stretch attack. Hence there is a large of energy loss. New protocol called PLGP, a valuable and secure protocol is proposed along with the key management protocol called Elliptic Diffie-Hellman key exchange protocol to avoid this vampire attack.

Savitha.M,Dr. R.Manavalan [11] "Efficient Data Transmission Using Energy Efficient Clustering Scheme for Wireless Ad- Hoc Sensor Network" in this title we have discuss In WASN, secure routing protocols are used to protect against attacks. Partitioning the nodes into different cluster is one of the most effective methods to solve the problem of energy in Wireless Ad hoc Sensor Network. PLGP schemes with path attestations increase the size of each packet, incur penalties in terms of bandwidth use, and radio power. The Energy Efficient Clustering Schemes (EECS) is introduced for reducing the energy consumption of the Ad hoc wireless sensor network as well as prolong the lifetime of the networks and preserve a balanced energy expenditure of nodes network. Clustering is a technique which selects the number of cluster head depends upon cluster nodes energy and the same is used to transfer the data.

3. PROPOSED SECURE IDS ROUTING

In this section describe however the module work and to safeguard our information from evil spirit attack. In data format part offer the knowledge concerning initial variable that used for reasoning the knowledge concerning evil spirit attack and its bar. Afterward we tend to decision route request part exploitation AODV (Ad-hoc on demand distance vector routing) and notice the behaviors of evil spirit and conjointly analyze the energy gain by the evil spirit attack. whereas wrongdoer node detected then we tend to goes into the bar part and block the wrongdoer node or modification standing into traditional condition by wrongdoer, therefore no hurt in future information and energy utilization solely by the desired zone. That mechanism decreased the energy conservation by the wireless device nodes and conjointly defends by evil spirit attack.

```
W: set of sensor nodes
S: set of sender nodes ϵ W
R: set of receiver nodes ϵ W
AODV: Routing protocol
E: energy of node
V: vampire node
P: protector node
Call-rreq-bcast(S,R,E,AODV)
    If (route exist from S to R && hop-count > 1)
    {
Intermediate node exist
Reply R to S for data sending by the fresh established path
If (intermediate status is abnormal)
    {
    Identify their abnormality
If (abnormal == drop packet || unwanted packet spread|| route update)
    {
    Gain energy of sender and other nodes
    Watch by IPS node
    }
            }
    Else if (intermediate status is normal)
    {
    No any attack
    Send data through that path
                        }
            }
IPS (neighbour info, abnormal status, node no, energy info of abnormal node)
    {
If (IPS receives abnormal information by any neighbour)
    {
Unicast normal status change message to attacker node
If (status not changes)
    {
Broadcast abnormal information to all alive nodes
Block the attacker node
    }
    Else if (status change as normal)
    {
    Path is future established
    Watch attacker node by IPS
    }
    }
    }
Stop
```

4. SIMULATOR OVERVIEW AND PERFORMANCE MEASUREMENT

Network Simulators area unit comparatively quick and cheap as they permit the engineers to check eventualities which may be notably tough or big-ticket to emulate exploitation real hardware. The instance of is simulating the consequences of a packets consumption or attack on a network service. These permit designers to check new networking protocols or amendment the present ones during prohibited surroundings.

The simulation can do on the Network machine a pair of (NS2) is that the results of associate degree on-going effort of do analysis and growth that's administrated by researchers at Berkeley [12]. NS began as a variant of the important network machine in 1989 and has evolved considerably over the past few years. In 1995 ns development was supported by DARPA through the VINT (Virtual lay to rest Network Testbed) project at LBL, Xerox PARC, UCB, and USC/ISI. it's a separate event machine targeted at networking analysis. Network Simulation may be a technique wherever a program models the network behavior either by hard the interaction between the various network entities by really capturing and enjoying back observations from a production network.

A. Simulation Parameters

The simulation parameters are mentioned in table1. These parameters are also change based on requirement so, in this table the following parameters are considered in this research.

Table 1: Considered Simulation Parameters

Simulator Used	NS-2.31
Number of nodes	50
Dimension of simulation area	1000m×1000m
Routing Protocol	AODV
Simulation time	100 sec.
Traffic type (TCP & UDP)	CBR (5pkts/s)
Packet size	1024 bytes
Number of traffic connections	6
Node movement at max Speed	random (30 m/s)
Transmission range	250m

B. Performance Metrics

There are following different performance metrics [4] has been considered to make the comparative study of these routing protocols through simulation.

1) **Packet Loss Percentage:** Rate of infection in network due to attacker or malicious nodes w.r.t time.

2) **Routing overhead:** This metric describes how many routing packets for route discovery and route maintenance need to be sent to propagate the data packets.

3) **Average Delay:** It indicates how long it took a packet to travel from the source to the application layer of the destination. It is measuring in mille seconds.

4) **Throughput:** This metric represents the total number of bits forwarded to higher layers per second.

5) **Packet Delivery Ratio:** The ratio between the amount of incoming data packets and actually received data packets.

5. RESULTS ANALYSIS OF NORMAL, MALICIOUS AND PROPOSED SECURE IDS ROUTING

The results analysis of normal routing, malicious attack and proposed secure IDS is illustrated the effect of Malicious bodes in routing.

C. Attacker Analysis

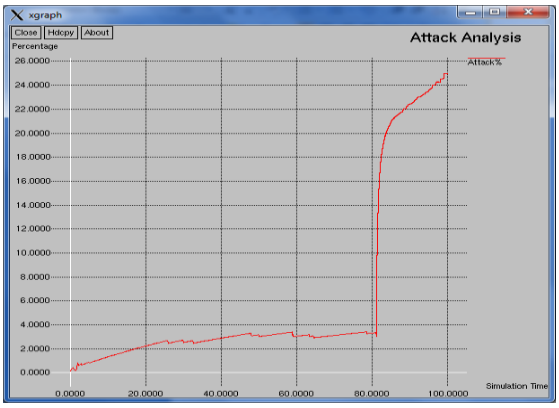

Figure1: Attacker Loss Percentage

This graph represents the infection percentage analysis in case of vampire attack. Here we clearly visualized about 25% network are only infected from attack. The infection in network is started at beginning of the simulation. The attacker is unnecessary consumes the nodes energy by that they are not working as they actually done in network. But after applying IPS scheme the infection are zero in presence of attack it means, the security scheme are completely block the misbehavior activity of attacker.

D. Attacker Identification and Drop Analysis

The number of nodes and that nodes are infected how many packets in network are mentioned in table2. The number of attacker nodes in network is 5, and these nodes in network are drops the data packets in network and ensured the unwanted consumption of nodes energy in network. The attacker 26 is flooding large number of packets and the nodes that are receiving that packets waste their energy for receiving. The percentage in data loss of attacker nodes is actually calculated w.r.t total data is received in network.

Table2: Attacker Nodes Identification

Vampire Node	Packet Capture	Percentage of Infection
12	93	0.01
17	112	0.01
26	226740	29.03
34	484	0.06
36	15012	1.92

E. Packet Delivery Ratio Analysis

The packet delivery ratio (PDR) analysis is measured through the packets percentage receiving at destination in a given simulation time in network. The percentage analysis is completely depending on the ratio of numerator and denominator. This graph exemplified the PDR analysis in case of normal energy routing, in presence of vampire attack and proposed IPS presence routing in network that secure the network from unnecessary energy consumption. The PDR in normal routing is about 90 %.

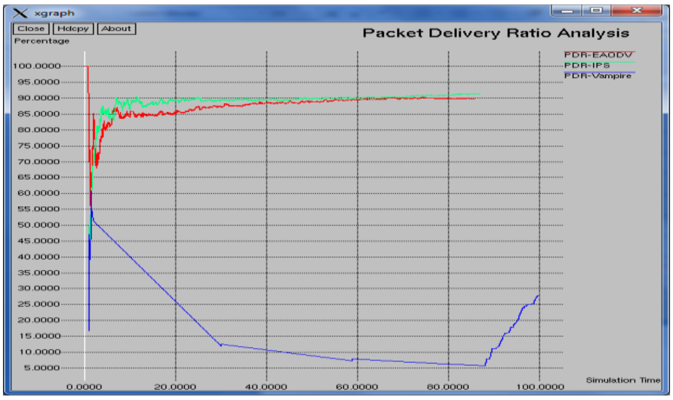

Figure 2: PDR Analysis

The attacker is degrades the network performance by that PDR value is not more than 25 percent but in case of proposed IPS it is about 90 % in network at the end of simulation. The minor difference is represents that the improvement in percentage of data receiving. The proposed scheme utilizes the maximum amount of energy in data delivery in network by that the packets receiving is improves in network i.e. also enhance the network performance in presence of attacker.

F. Routing Packets Analysis

The routing load is measured in network on the basis of ratio of number of control packets and the data packets received in network in a given simulation time. The more number of data packets are showing the better performance in network but the packets receiving is down w.r.t. to control packets delivery then in that case more amount of control packets are required to deliver data to receiver. This graph exemplified the routing load or control overhead analysis of normal energy routing and proposed IPS with AODV routing protocol is almost equal about 4000 packets. The attacker is consumes the energy consumption in network by that the large amount of control packets i.e. about 160000 are deliver in network. That means the more amount of energy is consumed in network by that the routing overhead increases and limited battery power utilization decreases in network.

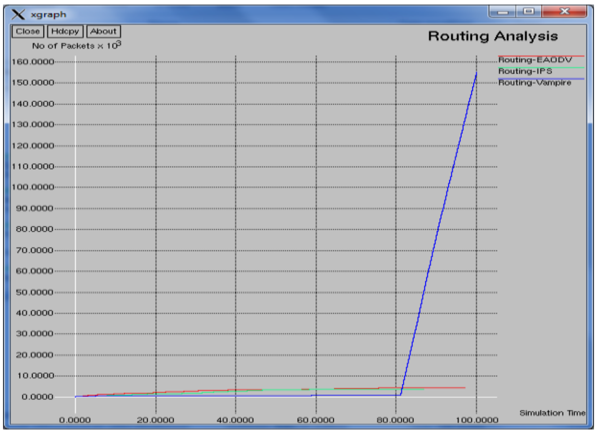

Figure 2: Routing packets flooding Analysis

G. Overall Summarized Performance Analysis of EAODV, Vampire Attack and Proposed IPS

The overall summarized analysis represents the exact network performance i.e. evaluated by performance matrices in case of normal AODV routing protocol with energy, vampire attack and energy efficient proposed IPS with AODV is mentioned in table 3. The performance of proposed IPS is much better in network because of utilizes the energy for data communication as equal to normal routing performance. The vampire attacker is really precarious that consumes the limited energy resource of other nodes. The attacker is nodes is identified by IPS and block their communication capability.

Table 3: Summarized Analysis

Performance Metrics	**EAODV**	**Vampire**	**IPS**
SEND	6020	1218	7320
RECV	5351	338	6639
ROUTINGPKTS	4486	155096	3860
Vampire Attack Pkt	0	242441	0
PDF	88.89	27.75	90.7
NRL	0.84	458.86	0.58
Average e-e delay(ms)	311.61	302.07	243.18
No. of dropped data (packets)	606	878	601

6. CONCLUSION AND FUTURE EXTENTION

In Wireless Sensor Network, two nodes communicate either directly or indirectly through other nodes and the aim is only one to deliver the data successfully in network. These nodes are typically powered by batteries with limited energy supply. The vampire attacker are consumes all energy of mobile nodes by that the network performance is really affected because of negligible packets receiving at destination end. When a node exhausts its available energy then in that condition it stops their functioning. This failure may potentially result in partitioning of the entire network. The limited battery bower in WSN is the crucial issue and their utilization is also necessary to improve the routing capability. Different study suggests different techniques to handle energy issue in different way. So this research effort is made a effort against vampire attack through proposed IPS. To reduce the energy consumption through proposed scheme attacker obstruction is necessary. The proposed IPS scheme aim is too totally removes the attacker power consumption of all nodes in the group i.e. minimizes the data packets loss, maximized the PDF and throughput that maximizing the life span should be considered. The node energy utilization is almost zero of some nodes because of fully affection from attacker. The attacker existence is identified by their infection percentage means data drop percentage e.g. shows zero in IPS presence. The simulation results are shows that the proposed scheme is minimizes the energy consumption and utilizes the energy for data delivery that enhances the network performance and degrades the possibility of link failure.

In future apply Global Positioning System (GPS) to trace attacker easily and also aware about the all nodes of network about malicious attacker. The proposed is also applied to flooding attack and measure routing performance.

7. REFERENCES

[1] Eugene Y. Vasserman And Nicholas Hopper "Vampire Attacks: Draining Life From Wireless Ad Hoc Sensor Networks" IEEE Transactions On Mobile Computing, Vol. 12, No. 2, February 2013.

[2] Gowrishankar.S, T.G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar "Issues in Wireless Sensor Networks" July 2 - 4, 2008, London, U.K.

[3] Eugene Y. Vasserman and Nicholas Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", IEEE Transactions on mobile computing, Vol. 12, No. 2, February 2013.

[4] Ankita Shrivastava, Rakesh Verma **"**Detection of Vampire Attack in Wireless Ad-hoc Network" international journal of Software & Hardware Research in engineering volume 1 issue jan-2015.

[5] Anoopa S, Sudha S K. "Detection and Control of Vampire Attacks in Ad-Hoc Wireless Networks" Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 4(Version 6), April 2014, pp.01-07.

[6] K.Vanitha,V.Dhivya "A Valuable Secure Protocol to Prevent Vampire Attacks In Wireless Ad Hoc Sensor Networks" IJIRSET Volume 3, Special Issue 3, March 2014.

[7] Gowthami.M, Jessy Nirmal.A.G,P.S.K.Patra "Mitigating Vampire Attack in Wireless Ad-Hoc Sensor Networks"IJARCST Vol. 2 Issue Special 1 Jan-March 2014.

[8] Ambili M. A, Biju Balakrishnan, "Vampire Attack: Detection and Elimination in Wsn" Volume 3 Issue 4 April 2014 ISSN NO 2277.

[9] Kirthika.K, Mr.B.Loganathan, "VAMPIRE ATTACKS IN WIRELESS SENSOR NETWORK –A SURVEY" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 7, July 2014.

[10] P.Rajipriyadharshini,V.Venkatakrishnan,S.Suganya,A.Masanam,"Vampire Attacks Deploying Resources in Wireless Sensor Networks" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 2951-2953.

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

[12] http://www.isi.edu/nsnam/ns/tutorial/index.html