ISSN:0975-9646

Secure Communication against Vampire Attacks in WSN (Survey)

Laxmi Choukiker
M.tech scholar

Amit Saxena
Associate Professor

Dr Manish Manoria
Professor

Department of CSE ,Truba Institute Of Engineering & Information Technology, Bhopal

***Abstract*— WSN is a group of wireless nodes in which each node communication with each other. Each sensor node comprises sense, giving out transmission, location finding structure, and control units. Sensor nodes are typically spread in sensor field, which is an area where the sensor nodes are deployed. Security is an important feature for the operation of wireless sensor network. In sensor system the attacker vampire attacks watch the whole system each node activity. In this paper we expected a protection scheme against attacker and false information of unique node. It means attackers are not drop the data packet of the node. The security scheme has showing the better performance of that is prove by simulation result. The security scheme has recovered the network presentation in company of attacker and offer attacks free network environment.**

Index Terms— WSN

I. INTRODUCTION

A wireless unexpected sensing component system consists of variety of sensors unfold across a geographic area. Every sensing element has wireless communication capability and a few level of intelligence for signal process and networking of the information. Sensors area unit unfold in associate setting with none planned infrastructure and get together to execute common observation tasks that typically consist in sensing setting information from the encompassing environment.

Wireless sensing element networks give distinctive opportunities of interaction between laptop systems and their setting. Their preparations are often delineate at high stage as follows: The sensing component nodes live environmental characteristics that area unit then processed so as to notice events. Upon event finding, some actions area unit triggered.

This terribly general picture applies to very security vital military applications moreover on such kind ones. One of the most style problems for a sensing element system is conservation of the energy out there at every sensing element node. The energy potency of a joint is outlined because the magnitude relation of the number of knowledge delivered by the node to the full energy gone.

Higher energy potency implies that a larger variety of packets are often transmitted by the node with a given quantity of energy reserve. Adversary injecting malicious info or sterilization legitimate routing setup messages, or will forestall the routing procedure from functioning properly. As an example, associate aggressor will forge messages to convert legitimate nodes to route packets during a method from the right destination. Evil spirit attack is one among the resource depletion attacks. The resource depletion attack focuses the node’s batteries life. Vampire attacks have an effect on any protocol and utilize the properties of routing protocols categories like supply routing, distance vector and link state and geographic and beacon routing.

II. APPLICATIONS OF WIRELESS SENSOR NETWORKS

A. Military or Border control investigation Applications WSNs are getting associate integral a part of military command, control, and communication and intelligence systems. Sensors will be deployed in a very battle field to observe the presence of forces and vehicles, and track their movements, facultative shut police work of opposing forces

B. Environmental Applications Environmental applications embrace following the movements and patterns of insects, birds or little animals.

C. Health Care Applications Wireless device networks will be accustomed monitor and track elders and patients for health care functions, which may considerably relieve the severe shortage of health care personnel and scale back the health care expenditures within the current health care systems. For instance sensors will be deployed in a very patient’s home to observe the behaviors of the patient. It will alert doctors once the patient falls and needs immediate medical attention.

D. Environmental Conditions watching WSN applications during this space embody watching the environmental conditions moving crops or ethereal mammal, watching temperature, wetness and lighting in workplace buildings, and so on.These watching modules might even be combined with mechanism modules which might management, for instance, the quantity of chemical within the soil, or the quantity of cooling or heating in a very building, supported distributed sensing element measurements.

E. Home Intelligence Wireless sensing element networks will be accustomed offer a lot of convenient and intelligent living environments for personalities. for instance, wireless sensors will be accustomed remotely browse utility meters in a very home like water, gas, electricity then send the readings to a foreign centre through wireless communication.

F. Process management in business, WSNs will be accustomed monitor producing method or the condition of producing instrumentality. For instance, chemical plants or oil refiners will use sensors to observe the condition of their miles of pipelines. These sensors are accustomed alert just in case of any failures occurred.

G. Agriculture exploitation wireless sensing element networks among the agricultural business is progressively common; employing a wireless network frees the farmer from the upkeep of wiring in a very tough setting .Gravity feed water systems will be monitored exploitation pressure transmitters to observe storage tank levels, pumps will be controlled exploitation wireless I/O devices and water use will be measured and wirelessly transmitted back to a central centre for request. Irrigation automation allows a lot of economical water use and reduces waste.

H. Structural watching Wireless sensors will be accustomed monitor the movement among buildings and infrastructure like bridges, flyovers, embankments, tunnels etc... sanction active Engineering practices to observe assets remotely while not the requirement for pricey web site visits, likewise as having the advantage of daily knowledge, whereas historically this knowledge was collected weekly or monthly, exploitation physical web site visits, involving either road or rail closure in some cases. it's additionally way more correct than any visual examination that will be applied.

III. Issues and challenges in designing WSN Node Fault Tolerance:

It is the most important challenge in planning WSN to form the system out there at the longer length once a number of the nodes is also faulty as a result of performance of network depends on its availableness. to form the service out there to an oversized extent, it's not plagued by any reasonably faults.

- Synchronization: clock synchronization is another issue in WSN. It’s a crucial service for Wireless sensing element network to synchronize all native clocks of nodes within the network to fulfill specific demand.
- Scalability: WSN is turning into in style thanks to it quantify ability feature. Sensing element network growing progressively as a result of sensors square measure low price devices and protocol support giant network It’s difficult to deploy wireless sensing element network to an oversized scale and work with efficiency with large quantity of nodes [2].
- Node Heterogeneity: wireless sensing element network could be a immense assortment of heterogeneous sensing element nodes. Every sensing element node includes a completely different ability, computing power and vary .It is tough to make sensing element network with heterogeneous node as compare to unvaried node.
- Security: Security is a crucial issue of wireless sensing element network .It is most tough to make WSN with security considerations like Data confidentiality: sensing element nodes don't reveal secret data to alternative nodes.
- Data confidentiality: sensing element nodes don't reveal secret data to alternative nodes.
- Data integrity: It assures that knowledge doesn't modification by adversaries throughout the transmission.
- Authentication: knowledge should be accessed by approved user.
- Data Freshness: It ensures that knowledge should not contain recent or previous knowledge.

IV. Security Threats in WSN

Wireless sensing element Network one in all the Denial-Of-Service attacks on routing procedure is resource reduction attack called a evil spirit attack. Battery power is a very important resource, every sensing element joint have rely upon the battery power for his or her work, however evil spirit attack eat the node’s battery and slowly disable the network availableness

Vampire attack: evil spirit attack could be a reasonably DOS attack. That during within which for the motion and causing of the message done by the malicious node in which causes a set of energy to be consumed.

It causes resource reduction (energy) at every sensing element nodes; by destroy battery control of each node. They are doing not disrupt the network availableness straight off, instead it compose a message with very little quantity of information and bigger energy drain. These work slowly over an extended amount of your moment in time and destroy the network services by exhausting the battery power of nodes.

It transmits small low grievance messages to stop a full network, thence it's terribly tough to diagnose and forestall [3]. Evil spirit attacks square calculate a network layer attack. they're not protocol-specific, therein they are doing not rely upon the planning properties or implementation details of exact routing protocols, however rather utilize common properties of protocol categories like link-state, supply routing, geographic, distance vector, and beacon routing.

Neither do these attacks rely upon Flooding the network with large amounts of information, however somewhat try and transmit as very little knowledge as potential to achieve the most important energy drain, preventing a rate limiting resolution

V. Related Work

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: Demanding Life from Wireless Ad Hoc Sensor Networks” This title explore resource reduction attacks at the routing procedure layer, which permanently stop networks by fast complex nodes’ battery power. These “Vampire” attacks are not exact to any specific procedure, but rather rely on the property of many popular program of routing protocol.

We find that all examine protocol are at risk to Vampire attacks, which are shocking, difficult to sense, and easy to hold out using as few as one wicked insider sending only protocol-compliant messages. In the worst case, a single Vampire can enhance network-wide energy procedure by a factor of O(N), where N in the number of network nodes.

We chat about methods to moderate these types of attacks, as well as a new proof-of-concept procedure that provably bounds the injure caused by Vampires during the packet forwarding phase.

Ankita Shrivastava, Rakesh Verma[4] "Detection of Vampire Attack in Wireless Ad-hoc Network" in this heading we explain a Vampire attacks alter 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 manage of Vampire Attacks in Ad-Hoc Wireless Networks"in this title we discuss work explores the classification of resource reduction attacks at the routing procedure layer and in the application layer, which eternally disable networks by quickly demanding nodes' battery control.

These Vampire attacks are not exact to a particular procedure, but quite rely on the property of many popular course of routing protocol It is clear that all examine protocols at risk to Vampire attacks, which are shocking, difficult to sense, and are easy to take out using as few as one hateful insider transfer only procedure compliant messages.

K.Vanitha,V.Dhivya [6] "A expensive Secure procedure to stop Vampire Attacks In Wireless Ad Hoc Sensor Networks" in this heading we have discuss Ad hoc require no centralized administration so the network infrastructure can be twisted quickly and inexpensive set up is needed. Ad hoc networks are person used in military operation, emergency disaster relief and community networking. An important security issue that has been recognized in these networks is resource drop attack at routing layer protocol. These attacks exhaust nodes battery power totally, so that the network is eternally disabled. Hence these attacks are term as vampire attacks.

Even as there exist many safe routing `procedure, they are not capable to defend the network from vampire attacks. So as an attempt to eliminate vampire attacks, three most important offerings 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 stand the attack by employ the Cluster Head. In case of each Vampire attack, the Cluster Head employ in this location and distributes the package to destination without dropping the packet. Thus give a successful and reliable message delivery even in container of Vampire attack. In the worst case, a single Vampire can add to network wide energy practice 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 antenna nodes. Energy is the one most important issue while considering sensor nodes.

Wireless sensor networks need solution for preserve energy level. One new type of attack called vampire attack, which happening at network layer. It leads to reserve reduction (energy) at each transmitter nodes, by destroy battery power of any node. It transmit a small complaint messages to disable a whole network, hence it is very hard to detect and prevent.

Existing protocol are not focus on this vampire attack occurrence on routing layer, hence there exist two types of attacks - carousel attack and stretch attack. Hence there is a large of energy loss. New protocol called PLGP, a expensive and secure protocol is planned along with the key organization protocol called Elliptic Deffi-Hellman key exchange protocol to avoid this vampire attack.

Savitha.M,Dr. R.Manavalan [11] "Efficient Data Transmission Using Energy resourceful Clustering Scheme for Wireless Ad- Hoc Sensor Network" in this name we have discussed In WASN, secure routing protocol are used to protect next to attacks.

Partitioning the nodes into different cluster is one of the most effective methods to solve the problem of energy in Wireless Ad hoc antenna Network. PLGP schemes with path attestations increase the size of each packet, incur penalties in term of bandwidth use, and radio power. The Energy Efficient Clustering Schemes (EECS) is introduced for reducing the energy use of the Ad hoc wireless sensor network as well as prolong the lifetime of the network and protect a balanced energy spending of nodes network.

Clustering is a technique which selects the figure of cluster head depends upon cluster nodes energy and the same is used to transfer the data. G. Vijayanand, R. Muralidharan [12] "Overcome Vampire Attacks trouble In Wireless Ad-Hoc Sensor Network By Using Distance Vector Protocols" In this paper the attacks which is mainly focus on routing protocol layer that type of attacker is known as resource reduction attacks.

This attack causing are the impact of persistently disabling the networks by drastically draining the node's battery control. These "Vampire" attacks are not impact any specific kind of protocols. Finding of vampire attacks in the network is not an easy one. It's very hard to detect, devastating .A simple vampire presenting in the system can increasing network wide energy usage.

We discuss some method and different routing protocols solution will be avoiding some sort of problems which causing by vampire attacks.

Meghana N Dr. G. F. Ali Ahammed [13] "A study on Vampire Attacks in Wireless Ad-Hoc Sensor Networks" This title explores resource reduction attacks at the routing protocol layer, which permanently disable networks by fast demanding nodes' battery power.

These "Vampire" attacks are not exact to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. We find that all examine protocol are at risk to Vampire attacks, which are shocking, difficult to detect, and are easy to carry out using as few as one terrible insider sending only protocol compliant messages.

In the worst case, a particular 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 moderate these types of attacks, including a new proof-of-concept protocol that provably bounds the break caused by Vampires during the packet forwarding phase.

Vasserman, and Nicholas Hopper [14] "Vampire attacks: Demanding life from wireless ad-hoc sensor networks" This paper explore resource decrease attacks at the routing protocol layer, which permanently stop networks by quickly draining nodes' battery power. These "Vampire" attacks are not exact to any exact protocol, but rather rely on the properties of many accepted classes of routing protocols.

We find that all examine protocol are subject to Vampire attacks, which are shocking, difficult to detect, and are simple to hold out using as few as one hateful insider sending only protocol compliant messages. In the worst case, a single Vampire can raise network-wide energy usage by a factor of O(N), where N in the number of network nodes.

We discuss methods to moderate these types of attacks, including a new proof-of-concept process that provably bounds to injure caused by Vampires during the packet forwarding phase.

VI. Problem Statement

Vampire attack happens within the system within the sense, any of the nodes within the system that is affected or infected and this nodes behavior is suddenly dynamic for the network behavior, this type of nodes area unit known as "Malicious node".

If malicious nodes gift within the system energy that are exploitation by every and each nodes can will be increase drastically. The malicious nodes are place within the system unambiguously. Initial In between the routing nodes, and therefore the second placed within the supply node itself. The possibility of putting a malicious join within the routing path this makes inflicting injury in network.

Supply node characteristic the actual packets and elect packets square measure known for the routing to the destination. The routing path is discovering by supply node by exploitation shortest path routing algorithmic program and therefore the path shouldn't be changeable by the intermediate nodes.

VII. Proposed Work

AODV belong to the category of Distance Vector Routing Protocols (DV). In an exceedingly DV each node is aware of its neighbor's and therefore the prices to get within the direction of them. A node maintain its own routing table, store all nodes within the network, the space and therefore the next step to them. If a node isn't approachable the space to that is about to time with no sign of ending. Each node sends its neighbor's sometimes its complete routing table. In order that they will check if there's a helpful route to a different node exploitation this neighbor as next hop. AODV is associate 'on demand routing protocol' with little delay.

VIII. Conclusion

This analysis is extremely helpful in field of engineering to guage the network presentation now in case of attack Wireless device network may be a quite ad-hoc network.

There a brand new quite internal attack known as vampire attack drain the energy of every device within the network, during this planned work a evil spirit attack is investigated and applicable methodology is planned for implementation for rising security and performance in network by distinguishing and removing suspicious join from the network supported the recently developed techniques a replacement security technique is meant and enforced for simulating the impact of attack preparation and as a result the performance improvement once security theme implementation. In addition, for justifying the answer and their improved performance ancient routing protocol is needed to check with the developed routing protocol.

In terms of outturn, finish to finish delay, stay energy and packet delivery magnitude relation. In future we tend to implement our planned Technique in NS2 and find malicious node that causes vampire attacks and take lost the vampire node from the network. We have a tendency to conjointly compare our planned work with Existing work.

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] G. Vijayanand, R. Muralidharan "Overcome Vampire Attacks Problem In Wireless Ad-Hoc Sensor Network By Using Distance Vector Protocols" International Journal of Computer Science and Mobile Applications,Vol.2 Issue. 1, January- 2014, pg. 115-120.

[13] Meghana N Dr. G. F. Ali Ahammed "A Survey on Vampire Attacks in Wireless Ad-Hoc Sensor Networks" International Journal of Advanced Research in Computer Science and Software Engineering 5(5), May- 2015, pp. 828-830.

[14] F.L. Lewis, "wireless sensor network," Technologies Protocols and Applications, New York, 2004.