ISSN:0975-9646

A Secure Ad hoc Wireless Sensor Network For Vampire Attack

Deepmala Verma[#1], Gajendra Singh[*2], Kailash Patidar[#3]

[#]PG Scholar, Dept of CSE, ShriSatyaSai Institute of Science & Technology, Sehore
**Professor, Dept of CSE, ShriSatyaSai Institute of Science & Technology, Sehore*
**Asst. Professor, Dept of CSE, ShriSatyaSai Institute of Science & Technology, Sehore*

Abstract—**Wireless sensor network is new generation application and information sensing network technology. Ad hoc nature of network adds advantages on the network due to rapid installation, low cost, freedom of mobility. Due to this nature of network the network faces security issues because malicious user can join the network. Thus security is a key area of concern in network technology, most of the time malicious user utilizes the network routing protocol information and creating issues during normal function of network. In this presented work the security is of wireless sensor network is investigated under the vampire attack. The vampire attack is a kind of attack model that can be deployable with any kind of protocols. Therefore it is a serious condition for network, in most of cases the attacker making effort for consuming the energy of network nodes. This causes hurdle in normal functioning of network. Additionally that is also increases routing overhead of the network by which the performance of network get affected. In order to prevent the malicious attacker in network a strong routing technology is required to develop which prevent attacker during the route discovery in network. Therefore a two stage malicious node prevention technique is developed in this work. In first phase the network nodes are classified as the suspected node and legitimate node and further the suspected node is again classified as the malicious node and legitimate node. For implementing the desired technique the AODV routing protocol and NS2 (network simulator 2) is suggested. After implementation of the proposed technique the security and performance is measured and compared with the traditional routing protocol. The comparison of both the network routing protocols are performed on the basis of packet delivery ratio, energy consumption and the RREQ flooding. According to the obtained results the performance of the proposed vampire attack prevention technique is found optimum and efficient as compared to the traditional routing protocol.**

***Keywords*— wireless ad hoc networks, routing algorithm, vampire attack, resource consumption, results analysis**

I. INTRODUCTION

A wireless sensor network is a distributed real-time system. Unfortunately yet very little work is applied in these new system and always a new solutions are often essential in all areas of resource consumption attacks. The main cause is that the set of assumptions underlying earlier work has changed dramatically. Most of the earlier distributed systems research works on the following assumption like the systems are wired; powers is unlimited, not works on real-time, with a fixed set of resources, have user interfaces such as screens and mice, treat each node of the system as very significant and are location independent. In contrast, the designing of a wireless sensor network should be formulated with keeping following terms in consideration such as the systems is completely ad-hoc and works with wireless channel, have scarce power, are real-time, utilize the sensors and actuators as interfaces, with dynamically changing sets of resources, aggregate behaviour is also important there and location is very critical. Various wireless sensor networks also exploit negligible capability devices which places a further strain on the ability to use precedent solutions.

As discussed the wireless sensor network is a collection of sensing nodes and they are connected through the wireless links. In this network the density of node is higher and the resources are limited such as CPU and energy. Therefore during design of the sensor network the key aim is to preserve the network resources in terms of energy and CPU. But the mobility added networks reflect additional aspects for design such as connectivity and the losses during the communication sessions. In order to preserve the performance of network the routing strategy is developed to ensure the effective route discovery and maintenance. During investigations that are obtained the routing protocols are weekly designed for adopting the mobile sensors activity. Due to this attacker can also join the network and harm the network performance.

In this presented work the key aim is to investigate the wireless sensor network and their performance issues due to the malicious activities in network. Therefore the discussed attack model in [2] is utilized for study. During the study it is observed the vampire attack is a much serious attack which can be deployed through any kind of network protocol and can damage the network performance in terms of energy. If any sensor node’s energy is bellow then predefined thresholds then the sensor nodes are not functioning appropriately. Thus the attacker tries to consume the energy of the nodes in network by which network is stop proper functioning.

This section provides the basic description of the presented study work and the next section describes the targeted issues and challenges to design a secure and efficient routing protocol for preventing the vampire attack.

II. PROPOSED WORK

There are a number of issues observed during study of vampire attack investigation but here only the targeted issues are discussed for a novel solution development. Thus there are only two main issues of vampire attack deployment are described as:

Basically vampire attack is a variant of DDOS attack, which performs resources consumption on neighbour nodes. Therefore during the vampire attack targeted packets are modified for preparing long routes or misguiding the packets. In addition of that the malicious nodes are making frequent connectivity from the entire neighbour nodes in network using false control message exchange. Due to these neighbour nodes replies the false request for connectivity and draining energy rapidly. Therefore in order to detect and prevent the malicious nodes in network a new kind of scheme is required which monitor the network node's activity and provide the decision for maliciously behaving nodes.

On the other hand the malicious host only change a few information of the packets thus it is difficult to locate on network. Additionally during such kind of attack deployment the other network performance parameters like PDR (packet delivery ratio) and the Routing overhead not much effected thus when an attacker node penetrate the security is not identifiable. Thus detecting such kind of malicious host is a complex issue.

In order to provide solution for the vampire attack a number of new and recently developed solutions are available. But most of them are activated after affecting the network. Thus for developing the solution during route discovery phases a two phase discovery process is proposed in this work. In first phase the entire network nodes are classified into suspected nodes and legitimate nodes and after that the suspected nodes are evaluated to identify the actual malicious node that is damaging the network.

Suspected node discovery

In order to identify the suspected node thresholding concept is utilized for trust estimation. Therefore vampire attack's key property is utilized for estimating the decisional threshold. Basically in ad hoc networks the route discovery is utilized for establishing the communication sessions. Malicious user utilizes the RREQ flooding to establish the malicious connections. Due to this target node flood the packets further and drain their energy and performance in network. Thus first of all a normal network is created which not contains any malicious user in network using this number of broadcast in network is counted and a threshold value is determined. Using the given formula

$$threshold = \sum_{i=1}^{N} \frac{number\ of\ broad\ cast}{N}$$

This threshold value is used to mark the node suspicious.

Classification of Suspected node

Now after preparing the threshold value the malicious node is introduced in network when malicious node start functioning in network a sampling operation is performed on network. In this operation each nodes number of broadcasted packets are compared with estimated threshold value. The classification is taken place in the below given steps.

Suspected node classification

```
For each node in network
    If node. broadcast> threshold than
        Label node as suspicious
    Else
        Legitimate
    End if
End for
```

Table 1 suspected node classification

Malicious node discovery

After classifying the nodes in two groups the suspicious nodes and legitimate nodes required to remove the actual malicious nodes from network. In order to ensure the network damaging node a new kind of thresholding is utilize. Thus to estimate the second threshold value the nodes packet delivery ratio is considered which are suspected during first classification. To create such threshold during communication sessions suspected nodes average packet delivery ratio is considered and formulated as.

$$PDR_t = \sum_{i=1}^{N} \frac{PDR}{N}$$

After creating threshold using the normal nodes and suspected nodes each suspected node is tested through the normal nodes packet delivery ratio. If the suspected node's packet delivery ratio is higher or equal to normal nodes packet delivery ratio then the node is removed from the suspected node's list otherwise this node is removed from the network and labelled as the malicious node. The process of classifying the malicious node in network the process is given as:

Malicious node classification

```
If suspicious nodes PDR < normal nodes PDR
    Remove node
Else
    Label normal
End if
```

Table 2 malicious node classification

III SIMULATION SETUP

In this section provides the desired network configuration for simulation of proposed security scheme for security implementation against the vampire attack and simulation.

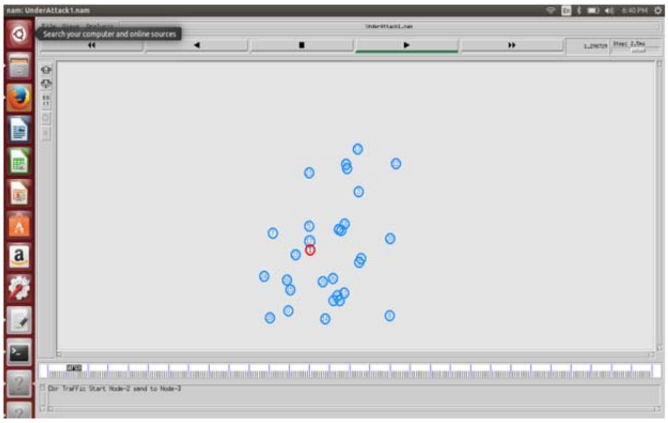
Simulation properties	Values
Antenna model	Omni Antenna
Dimension	750 X 550
Radio-propagation	Two Ray Ground
Channel Type	Wireless Channel
No of Mobile Nodes	30
Routing protocol	AODV
Time of simulation	30.0 Sec.

Table 3 Simulation Setup

In order to demonstrate the effect of vampire attack in wireless sensor networks two basic simulation scenarios are suggested to implement. Both of them are discussed as follows:

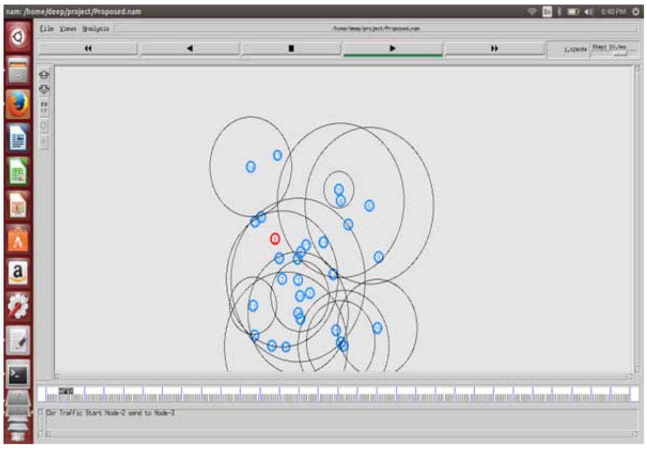
1. Simulation of wireless sensor network under attack situations: in this simulation scenario a wireless network is implemented using the NS2 simulator and using the AODV routing protocol. After the network preparation a malicious node is deployed on the network this simulation is used demonstrate the effect of vampire attack thus after simulation the performance of network is estimated. The implemented simulation is demonstrated using the figure 1 in this diagram the blue node shows the normal functioning node and the red node shows the malicious node in network.

2. Simulation of the proposed secure routing strategy under attack: the simulation of the proposed secure mechanism for vampire attack detection and prevention is demonstrated in this simulation. In order to prepare the simulation the wireless sensor network is implemented with the modified AODV routing protocol for preventing the effects of the Vampire attack and their simulation is given using the figure 2 in this diagram the normal functioning nodes are demonstrated using the blue nodes and the malicious node namely vampire node is simulated using the red node.



Cbr Traffic Start Node-2 send to Node-3

Figure 1 first scenario


nam: /home/deep/project/Proposed.nam
File Views Analysis
/home/deep/project/Proposed.nam
6:40 PM

Cbr Traffic Start Node-2 send to Node-3

Figure 2 proposed secure technique

IV Results analysis

The implementation of the secure routing technique with the help of previously defined AODV routing is performed successfully after that the network performance is evaluated under attack conditions for both the simulation scenarios. This section provides the detailed reporting about the obtained results in terms of different performance parameters.

Route request

During the ad hoc communication sessions when the source node required sending data then the route request messages are broadcasted first for route discovery. That is necessary but the continuous flooding of RREQ (route request) packets increases the routing overheads of the network. The comparative number of flooded RREQ packets is given using the figure 3 in this diagram the red line shows the amount of RREQ flooded when attack is deployed on normally configured network and the green line shows the RREQ flooding during the secure routing technique. according to the comparative outcomes the proposed secure technique requires the less number of packet exchange during initiation of communication but the normal network needs more packet flooding thus the routing overhead of the proposed technique is much effective than the normal network. thus proposed technique is efficient and effective as compared to traditional networks.

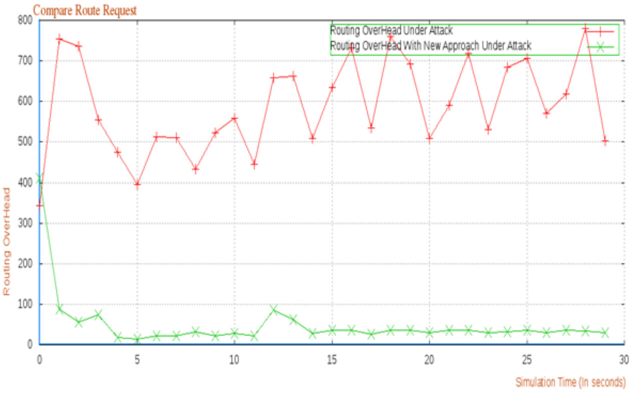


Figure 3 route request

Packet delivery ratio

The performance parameter Packet delivery ratio sometimes termed as the PDR ratio provides information about the performance of any routing protocols by the successfully delivered packets to the destination, where PDR can be estimated using the formula given

$$packet\ delivery\ ratio = \frac{total\ delivered\ packets}{total\ sent\ packets}$$

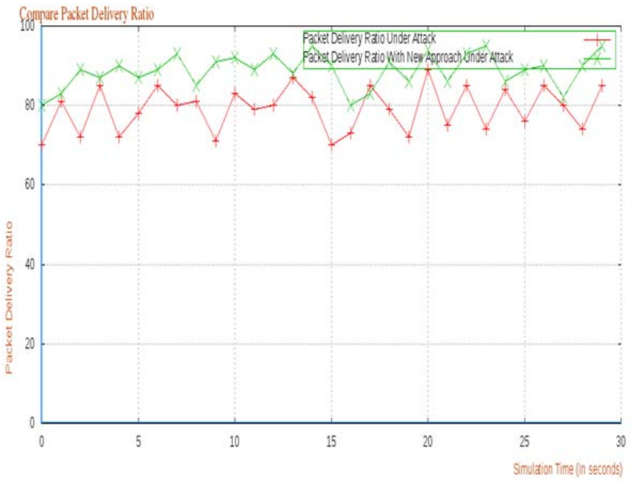


Figure 4 packet delivery ratio

The comparative packet delivery ratio of the proposed technique and normally configured network is given using figure 4 in this diagram the red line shows the performance of normal network and the green line shows the performance of the proposed routing technique. According to the obtained results the performance of the proposed routing technique is comparatively higher as compared to the normal network. For demonstrating the performance of the network the X axis shows the simulation time of the network in terms of seconds and the Y axis contains the amount of packet delivered to the destination.

Energy consumption

The amount of energy deduced from initial energy of nodes during the active communication sessions of network is known as energy consumption. The given figure 5 shows the energy consumption of both the networks under attack conditions. For demonstrating the results the X axis of the figure contains the simulation time in terms of seconds and the Y axis shows the amount of energy consumed with time in terms of Jules. The proposed techniques performance is reported using the green line and the red line shows the energy consumed with the normal network. According to the obtained results the performance proposed technique is preserve more effectively as compared to traditional network.

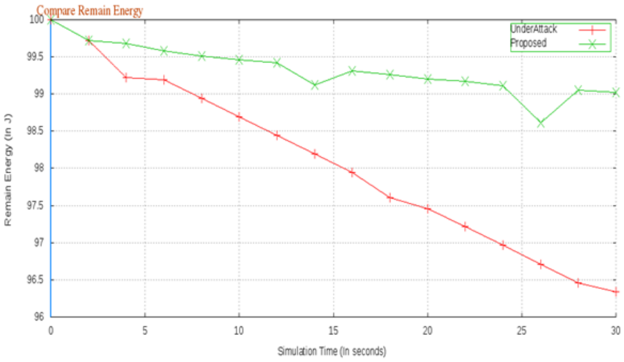


Figure 5 energy consumption

This section provides the results analysis and their understanding in next section the conclusion and future extension is reported.

V. CONCLUSION AND FUTURE WORK

Wireless sensor network is one of the most essential network technologies among different ad hoc networks. The ad hoc term is added to show the mobility and diversity in network and network topology. The network topology development and maintenance is key responsibility of network routing protocols. On the other hand most of the attacks in network is deployed using the routing technology and by modification. In addition of that the wireless network suffers from the security and performance issues among them the vampire attack is much effective and resource consuming attack for wireless sensor network.

In this attack the attacker consumes the network node's energy by frequent flooding of network request packets. Thus the deployment of the attack is less complex as the detection process. In literature a number of recently developed techniques and algorithms are available which are claimed to detect and prevent the malicious attacker in network. But most of them are not much effective or detecting the attacker when the attacker affects the network. Thus need to remove the attacker during the route discovery phases. Thus a new technique is proposed in this work which detect the malicious node during the route discover phases.

In order to develop the solution for the vampire attack a two phase classification approach is suggested to implement. In this approach the network node is first classified into two classes first the legitimate nodes and the suspected nodes using the RREQ flooding based thresholding and after that the suspected nodes are again evaluated using the PDR based threshold and the suspected nodes are classified into the malicious node and the normal functioning nodes. In order to implement the proposed method a traditional routing protocol namely AODV routing protocol is used. Additionally for implementation of the desired technique using AODV routing protocol the NS2 (network simulator 2) is used. After experimentation with the implemented routing protocol the performance of the network is evaluated in terms of different performance parameters and summarized using a summary table as given in table 3.

S. No	Parameters	Proposed	Traditional
1	RREQ flooding	Low	High
2	Energy consumption	Low	High
3	Packet delivery ratio	High	Low

Table 3 performance summary

According to the obtained performance the proposed secure routing protocol provides the efficient and secure routing as compared to the traditional approach of wireless sensor network routing protocols.

The key aim securing wireless sensor network under the vampire attack is accomplished successfully. The proposed technique provides an energy efficient and secure routing for wireless sensor networks. But the presented solution optimizes the energy consumption and provides the security using only two basic parameter consideration. In near future that is required to include more parameters for evaluating the suspected nodes for classifying as malicious node or legitimate node.

References

[1] ArchanaBharathidasan, Vijay AnandSaiPonduru, “Sensor Networks: An Overview”, Department of Computer Science University of California, Davis, CA 95616.

[2] 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

[3] Paolo Baronti, PrashantPillai, Vince W.C. Chook, Stefano Chessa, Alberto Gotta, Y. Fun Hu, “Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards”, 2007 Elsevier B.V. All rights reserved.

[4] BhattuHarikrishna, Dr. Mohammed Abdul HaqueFarquad, “Wireless Sensor Network a New Paradigm for Sensing and Communicating the Communicating the Efficient Approach”, IJCSN International Journal of Computer Science and Network, Volume 3, Issue 4, August 2014

[5] Md. SirajulHuque, P. Anjaneyulu, A. Tirupathiah, “Secure Communications over Wireless Broadcast Networks Using Shortest Seek First Algorithm”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012

[6] Shio Kumar Singh, M P Singh, and D K Singh, “Routing Protocols in Wireless Sensor Networks – A Survey”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010

[7] Jamal Al-Karaki, and Ahmed E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey“, IEEE Communications Magazine, vol 11, no. 6, Dec. 2004, pp. 6-28.

[8] Kemal Akkaya and Mohamed Younis, “A Survey on Routing Protocols for Wireless Sensor Networks”, Ad hoc Networks, vol. 3, no. 3, May 2005, pp. 325-349

[9] N. Bulusu, J. Heidemann, and D. Estrin, “GPS-less Low Cost Outdoor Localization for Very Small Devices”, IEEE Personal Communication Magazine, vol. 7, no. 5, Oct. 2000, pp. 28-34.

[10] K. Akkaya and M. Younis, "A Survey of Routing Protocols in Wireless Sensor Networks”, in the Elsevier Ad Hoc Network Journal, Vol. 3/3 ,pp. 325-349, 2005

[11] A. Abbasi, M. Younis, “A survey on clustering algorithms for wireless sensor networks”, Elsevier Computer Networks Computer Communications, vol. 30, pp. 2826-2841, October 2007.

[12] Prashant Kumar Maurya, Gaurav Sharma, VaishaliSahu, Ashish Roberts, MahendraSrivastava, “An Overview of AODV Routing Protocol”, International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.3, May-June 2012 pp-728-732

[13] B. Umakanth, J. Damodhar, “Detection of Energy draining attack using EWMA in Wireless Ad Hoc Sensor Networks”, International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 8- August 2013

[14] 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

[15] Jose Anand, K. Sivachandar, “Vampire Attack Detection in Wireless Sensor Network”, International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3, Issue 4, July 2014

[16] TruptiBorgamwar, KanchanDhote, “Minimize the Vampire Attack using WSN on Routing Protocol”, International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 Issue: 6

[17] Abdul RazakQureshi, Prof. R.K. Krishna, “Enhancing Energy Efficiency by Detecting and Protecting from Vampire Attack in Wireless Sensor Networks”, International Journal of Innovative Research in Advanced Engineering, Issue 5, Volume 2 (May 2015)

[18] Trupti A Borgamwar, KanchanDhote, “Review of Resist to Vampire Attack using Wireless Ad-hoc Sensor Network”, International Journal for Research in Emerging Science and Technology, Volume-1, Issue-4, September-2014

[19] Geethu Raj, Halice K Babu, “Provable Security Against Resource Depletion Attacks in Wireless Ad hoc Networks”, International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), Volume 3, Issue 3, March 2014

[20] Pritam M. Channawar, Dr. Y. V.Chavan, “Vampire Attack: Energy Efficient Trust Based Solution”, International Journal of Science and Research (IJSR), Volume 3 Issue 12, December 2014

[21] Dantam Ramesh, DasariKoteswaraRao, “Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor communication of Networks”, International Journal of Research in Computer and Communication Technology, Vol 3, Issue 9, September – 2014

[22] A. Anto Jenifer, V. Thangam, N. JeenathLaila, “Maintaining Lifetime of Wireless Adhoc Sensor Networks by Mitigating Vampire Attacks”, –International Journal for Innovative Research in Science & Technology| Volume 1 | Issue 9 | February 2015