Preventing Vampire Attacks to Save the Battery Life in WSN

Shweta Ghate
Department Of Information Technology
MIT College of Engineering
Pune, India.

Vivek Deshpande
Department Of Information Technology
MIT College of Engineering
Pune, India.

Anil Hiwale
Department Of Information Technology
MIT College of Engineering
Pune, India.

***Abstract*—Wireless Sensor Networks (WSN) contain wireless nodes which can be mobile or stationary and has very limited resources.These nodes are generally deployed in remote areas where they are prone to various attack. One of such attack is Vampire attack which means creating and sending messages by malicious node that causes more energy consumption by the network leading to slow depletion of node's battery life. It is impossible to recharge or replace the battery power of such sensor nodes. The proposed Group Key Authentication Against Vampire Attack (GKAVA) algorithm is used to detect and prevent the vampire attack and reduce the energy consumption.**

Keywords:-Ad-hoc networks, low-power networks, routing, sensor networks, wireless networks.

I. INTRODUCTION

Wireless Sensor network is the collection of many small devices, called nodes.These devices has capabilities to sense,process and communicate.Different nodes may have different ecological parameters such as humidity,temperature,pressure,noise level etc.As nodes are small devices they have the limitation of processing memory and battery.Because of their space compact and limited resource feature ,WSN is beign used widely in many applications[1].

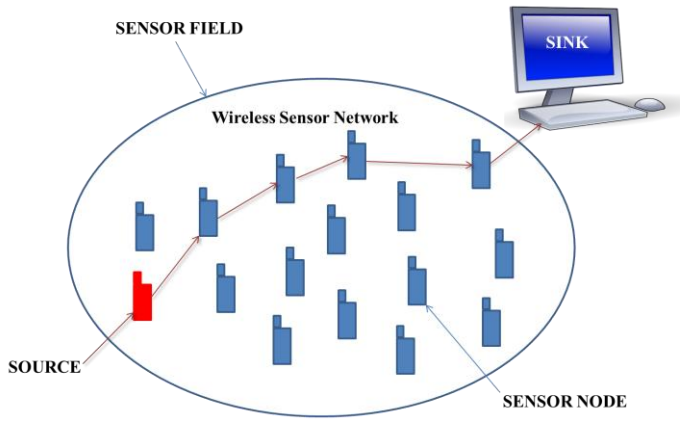

Figure 1: Wireless Sensor Network

Wireless Sensor Network is very effective to use in no man land or in remote areas where human intervation is very difficult .Because of these capabilities nowadays WSN is getting used in many of military applications.WSN needs security to enable its use in military application.[2]To provide security more processing power and memory is required.But because of its limited resource feature,wireless sensor network has attracted many researcher to provide the security feature with mininum resource utilization.

Figure 1 shows the wireless sensor network, which consist of number of sensor nodes.One of them are the source node which intiates the data flow in the network while other's are the forwarding nodes which used to forward the data to the sink.While forwarding the data integrity should be maintain untill it reaches to the destination,for that the WSN security should be taken into consideration.WSN is porne to various attacks like Denial of Service attack,blackhole attack,Jamming ,wormhole attack and many more[3].These attacks leads to loss of integrity,privacy and confidentiality of data. There are some major constraints in WSN such as energy,memory limitation,unreliable communication and higher latency in communication[4].To solve such kind of issuses researchers are still defining and proposing new methods.

The following paper provides the solution against the vampire attack which used to drain the battery of the node.There are two types of vampire attack i.e carousel attack and stretch attack.These paper shows the Group Key Authentication Against Vampire Attack (GKAVA) Algorithm which used to detect and prevent the vampire attack.

Further in paper, section II contains the literature survey,section III contains the proposed work and finally the performance analysis of the algorithm is shown along with the conclusion.

II. RELATED WORK

Eugene Vasserman and Nicholas Hopper[5] has disscuses about the battery draning attack called Vampire attacks.The attack in which the malicious packets are created and send by the malicious node which causes extra energy depletion by the network leading to slow exhaustion of node's battery life. Such type of attacks is called Vampire attack which sucks the battery life and disable the network. These are also called as resource depletion attack. Vampire attacks are not protocol specific,they don't disturb the immediate availability of the network.Vampire attacks use protocol complaint message,they

transmit little data with largest energy drain.These attacks are smart enough while sending data they do not distrupt or alter the discovered path.

To detect and avoid the vampire attack, the author have used the clean slate secure sensor network routing protocol(PLGP).This protocol has two phases i.e topology discovery phase and packet forwarding phase.In topology discovery phase the single node create the small group by merging and then this small groups merge and create the big network.Every node is having its own id and each group consist of its group id.At last in the topology discovery phase all node learns every other node's virtual address, public key, and certificate, as every group members knows the characteristics of all other group members and the network joins to a single group.In packet forwarding phase, all decisions are made freely by each single node[6].

The proposed algorithm PLGP has been tested in presence of the invader,but it shows some flaws.PLGP does not satisfies no-backtracking.PLGP was still susceptible to directional antenna attack and wormhole attacks,which allow opponents to divert packets to any part of the network. Thus to preserve no-backtracking,author have added a demonstrable pathway antiquity to each PLGP packet.PLGP with attestation(PLGPa) use this packet antiquity collected with PLGP's tree routing structure.But still this algorithm does not detect the invader in topology discovery phase[7].

S.H. Jokhoi et.all [8] have disscued about the node capture attack and they have anticipated a novel light-weight method called Sensor Node Capture Attack Discovery and Defense (SCADD) against the node capture attack in wireless sensor network.The procedure consist of two edifice chunks: node attack discovery block and defence supporting measure block. The earlier is responsible for strategic-based attack discovery to eradicate the probability of misjudgement.The second practices a self-destruction defence degree against node capture attack, without actually abolishing the node's wireless facility, to evade a chief safety gap.

Node capture attack happens due to lack of physical security of sensor nodes futher which leads to a unadorned danger of safety gap.Due to this attack there is also chances of revelation of the safety algorithm or undisclosed cryptograohic keys.The suggested procedure contains two blocks: node attack discovery block and defence supporting measure block which has specific working to detect and provide the defence against the attack[9].The node attack discovery block is used to identify the state and severity of the attack on a sensor node.And the defence supporting measure block is used to take the protective actions against the att ack.The proposed method provides the cost effective solutions.

Wenjun Gu et.all [10]has defined a procedure called distinguished key pre-dissemination to protect end to end communiqué in arbitrarily positioned wireless sensor network.To boost the resilence of the links,they have distributed different number of keys to different sensors.Applications like military,emergency and surveillance make use of wireless sensor networks,where the sensed data is send to the destination by the sensor node. But in many application it is difficult to deploy the sensor node deterministically so thus deployed arbitrarily.Eventually the problem regarding to end to end delay has been ignored normally[11].For that two methods has been proposed which provide high degree of end to end secure communication in wireless sensor network.The prior thing is to distribute the pairwise key to the sink as well as each sensor node so that each sensor node will encrypt the data using pairwise key and send the data to the sink.Its generally belive that end to end secure communication can be achieve by providing hop by hop encryption /decryption.That's why the next thing is to simply provide the hop by hop secure communication between neghbouing nodes.

R.Abirami and G.Premalatha[12] has proposed an protocol to save the network against vampire attack.They have proposed a Internal Gateway Routing Protocol to deplet the vampire attack in medium access control level.Vampire attack is a type of DOS attack which create harm to the network.IGRP is one of the distance vector routing protocol.It uses five standards to define the best path : the link speed,suspension,packet size,packing and dependability. IGRP use to discover and diminish the attacks made during message passing.It can avoid the attack by removal of attacked file going into the node from the source.It also certificates multipath routing.To define the best path IGRP uses Bellman-Ford algorithm[13].IGRP shows periodic routing update every 90 seconds for security purpose.As this protocol permits multipath routing it is design to enhance its steadiness and elasticity.The disadvantage of the method is that it does not handel the mobile network,derivation of damage bound and defence for topology discovery is still left.

Sunil Bhutada et.all[14]have proposed a new method to improve the life of network.They have proposed a new approach for secure routing protocol against vampire attack.In this method the vampire attack is detected at the destination. The proposed method work in four steps : first step is to generate a secured path for data transmission,secondly to do steps for key management,then to identify the invader in the network finally to track a path for presence of the attacker node.

In first step we have to forward the data securely.Here the author have used the clean slate sensor network rouring protocol (PLGP).In this protocol the data is forwarded in two steps : first by topology discovery phase and packet forwarding phase.Primarily the network is created in topology discovery phase and the data is securely forwarded in the packet forwarding phase.While forwarding the data we have to encrypt the data with the cryptographic key.For that key management has to be done, so in this key management stage here the author have used the elliptical curve cyptography.They use elliptical curve cryptography because it has small key size and hence use less memory and computation cost.After this it is important to find whether if there is any invader still present in the network.To solve this

problem the data is sent on the suggested path and hence the vampire attack like carousel attack and stretch attack are detected.As the data reaches at the destination it is necessary to find that whether the data is traversed the correct path[15]. To check the data traversal from the correct path ,each node maintain a log file,which conatins the history of the path , which the packet has traversed.The advantage of this protocol is ,it alleviates the vampire attack by saving bandwith ,energy and time period.This protocol is only used for the fixed network.

III. PROPOSED WORK

To prevent the network from vampire attacks we brought up new algorithm "Group Key Authentication Against Vampire Attack Algorithm" that can reduce the energy utilization of nodes and increase the lifetime of networks. The proposed algorithm comprises of three phases which are explained below

Phase 1:Pre-Deployment Key Distribution

This phase ensures the WSNs that; the attacker node will never have the keys that the honest nodes will use for communication. In this particular phase, the WSN is divided into '*k*' number of virtual groups. And each group is assigned with a Group ID, 'G_i'. Each node is then assigned with a set of public and private keys of other nodes. Also, the public and private key of the same group is also assigned to the node. The public key of other groups is also assigned to the node.

Phase 2: Network Discovery

This phase ensures that all the nodes will know their neighbouring nodes. And will attest the packets with their private and public keys. This attestation ensures that the malicious nodes will never be able to encrypt the packets with these keys. And such packets will easily being caught.

For the purpose of packet forwarding in the network the discovery of neighbour nodes is important for every node. Thus, in this phase, every node sends out a merge request to all the other nodes in the network. According to this merge requests, the groups are created. The merge request includes the Node ID and Public Key of Node encrypted using the Private Key of Group and the Group ID.

Phase 3: Packet Forwarding

This phase actually works on the forwarding of the packets and detection of the malicious nodes. As explained below.

-Every intermediate node is supposed to make the attestation of each packet it forwards. The attestation is nothing but the signature which contains the packet history of all packets it traversed.

-Then, every receiver node first extracts the source address from the message. This is to ensure whether the sender is an honest node. Later, it checks the attestation of the packet. If any of them is not valid, the network will simply drop the packet.

-In addition, each node will check the previous node, who has forwarded the message, and check if it is neighbour. And also checks, if the packet is progressing towards the destination. If not, then packet will be dropped.

If all condition satisfies, the node will find the next closest node to the destination. Then, it will append the attestation to the packet and forward it.

Group Authentication Against Vampire Attack Algorithm(GKAVA)

Step1: Divide the nodes into virtual groups.
Step2: Groups and nodes must exchange the keys .
Step3: To find its neighbor in network merge request is sent by nodes.
Following steps are followed for data exchange.

-Excerpt the source address =>sou.
-Excerpt the attestation =>att.
-Check
-The source signature(sou).
-The attestation (att) is empty and the node is not a neighbor node of source(sou).
-The last attestation.

- drop the packet,if above conditions fail.

Step4 :-For every single node

Verify who is the previous node.
Verify that the node and the previous node are neighbor.
Verify if the packet is progressing.

- drop the packet,if above conditions fail.
Step 5: Find the nearest next node to source => nsou
Step 6: Attach the attestation of packet => patt
Step 7: Check if the node is neighbour node then forward (patt,nsou).
Step 8: Otherwise forward (patt, next hop to non-neighbour node).

IV. PERFROMANCE ANALYSIS

CASE I : Simulation scenario contains nodes, three sources and one destination node. Reporting rate is 10 packets per second. Density of the node varies from 5-25. All the nodes are static. It uses Clean Slate Sensor Network Routing Protocol with attestation (PLGPa) routing protocol .Random topology is used in this scenario.

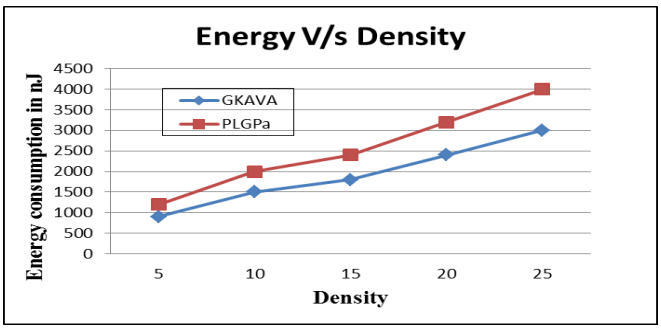

Figure 2: Energy as a function of Density

Figure 2 shows Energy as a function of Density. As the density of the nodes increases energy consumption increases for both the protocol. Both the protocols encrypt the data before sending, but in GKAVA the data is encrypted with ECC and on the contrary PLGPa uses AES for encryption of data. Computation required for ECC is less than that of AES. Hence the energy consumption by the GKAVA is less than PLGPa due their encryption techniques.

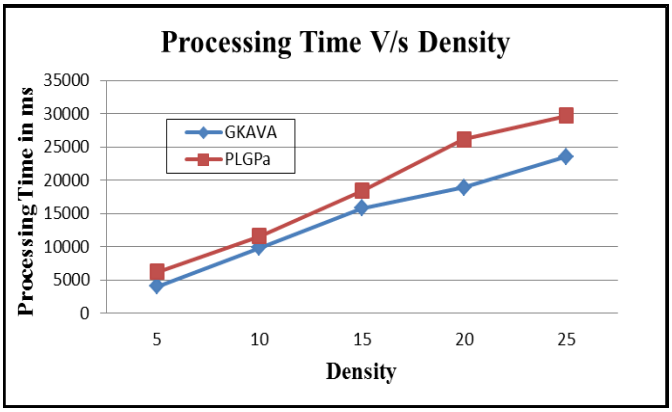

Figure 3: Processing time as a function of Density.

Figure 3 shows Processing time as a function of density of nodes in the network. As density increases processing time for both the protocol increases. As in GKAVA the data is encrypted with the elliptical curve cryptographic technique which has a better performance than that of AES technique used in PLGPa. So as a result the processing time required by the GKAVA is less than PLGPa.

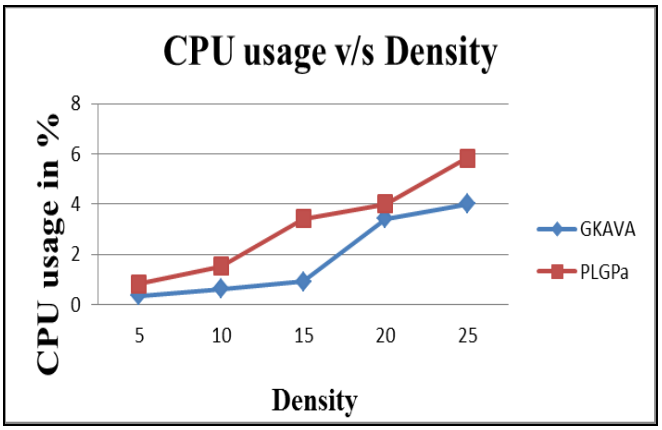

Figure 4: CPU usage as a function of Density

Figure 4 shows CPU usage as a function of density. As density varies the CPU usage goes on increasing for both the protocol. For Density 15 the graph shows maximum difference. And for density 20 the graph shows minimum difference .Overall for GKAVA the CPU usage is less than PLGPa.

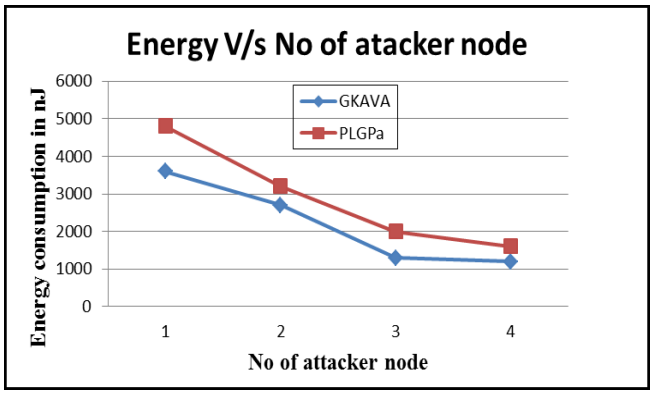

Figure 5: Energy as a function of Number of attacker node.

CASE II : Simulation scenario contains 20 nodes, three sources and one destination node. Reporting rate is 10 packets per second. The number of attacker node varies from 1-4. All the nodes are static. It uses Clean Slate Sensor Network Routing Protocol with attestation (PLGPa) routing protocol .Random topology is used in this scenario

Figure 5 shows the Energy as a function of number of attacker node in the network. Energy consumption decreases with the increases in attacker node in both the protocol. As number of attacker nodes increases malicious packets are thumbed into the network. The GKAVA algorithm requires less energy due to the use of ECC technique, whereas PLGPa uses AES for encryption which requires more energy than ECC. Hence the energy required by PLGPa is more than GAKVA.

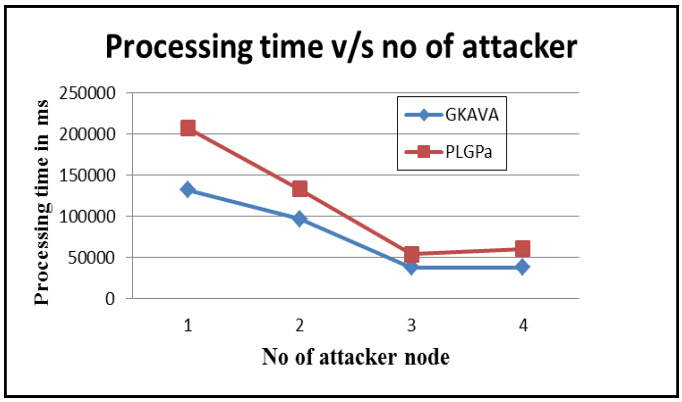

Figure 6: Processing time as a function of Number of attacker node.

Figure 6 shows the Processing time as a function of attacker node. As number of attacker node increases malicious packets are thumbed into the network. The graph shows decreasing result for both the protocol. The data is encrypted with the ECC technique in GKAVA algorithm and with the help of AES in PLGPa before sending. ECC requires less processing time than AES due to its small key size. Hence the processing time required by GKAVA algorithm is less than PLGPa as well as in case of normal network.

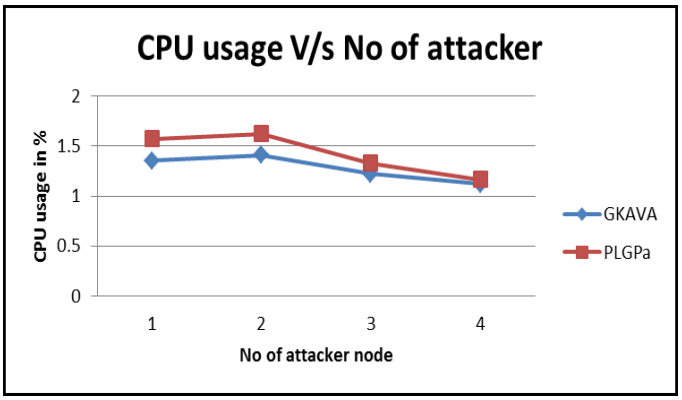

Figure 7: CPU usage as a function of Number of attacker node.

Figure 7 shows CPU usage as a function of number of attacker node .As no of attacker node increases there is decrease in the graph for both the protocol .While sending the data GKAVA use ECC technique for encryption on the contrary PLGPa uses AES technique. ECC requires less computation power than AES .Hence CPU usage for GAKVA is less than PLGPa.

CASE III : Simulation scenario contains 20 nodes, five sources and one destination node. Reporting rate varies from 15-55 packets per second. The number of attacker node varies from 1-4. All the nodes are static. It uses Clean Slate Sensor Network Routing Protocol with attestation (PLGPa) routing protocol .Random topology is used in this scenario

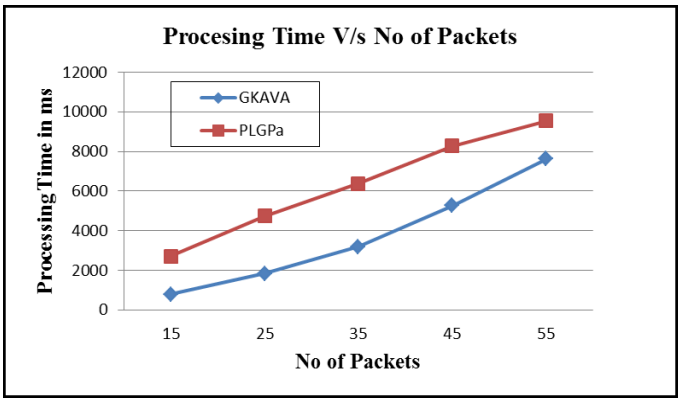

Figure 8: Processing time as a function of Number of Packets

Figure 8 shows Processing time as a function of number of packets. As the number of packets send by the source increases the processing time increases. The data in the packets are encrypted when they are sent. GKAVA algorithm encrypts the data using ECC technique which requires fewer cycles than AES technique used in PLGPa. Hence the Processing time required by the GKAVA is less than PLGPa.

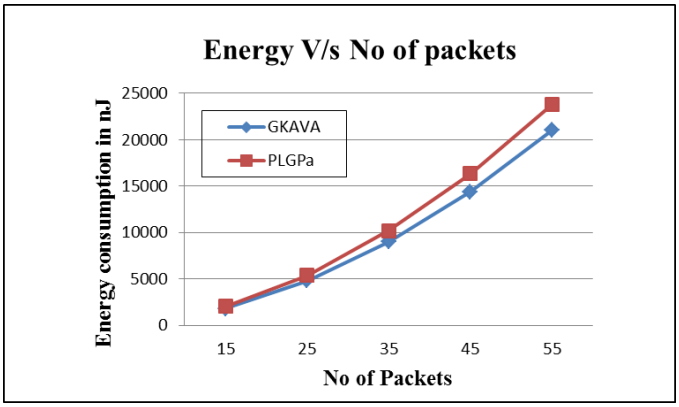

Figure 9: Processing time as a function of Number of Packets

Figure 9 shows Energy as a function of number of packets. Energy consumption increases with the increase in number of packets in the network for both the protocol. When the packets are forwarded in the network these packets are encrypted with the ECC technique in the GKAVA. On the other hand PLGPa uses AES for encryption of data. ECC use less cycles as compared to AES hence PLGPa consumes more energy than the GKAVA.

V. CONCLUSION

The comparative study and performance analysis of protocols (GKAVA and PLGPa) is done on the basis of energy consumption, processing time and CPU usage in presence of number of attacker node. The study of these protocols shows that GKAVA is more efficient in the presence of attacker node in comparison with PLGPa. Average energy consumption for GKAVA is 25% less than PLGPa. Processing time for GKAVA is 35% less than PLGPa. CPU usage for GKAVA is 10% less than PLGPa. As we vary the density the energy consumed by GKAVA is 25% less than PLGPa as well as the processing time required by GKAVA is 22% less than PLGPa. Similarly as the number of packets varies the energy consumed by GKAVA is 12% less than PLGPa and the processing time required by GKAVA is 47% less than that of PLGPa. Future work will include implementation of nodes on hardware device. Future work will also include the detection on attacker node in pre-deployment phase.

REFFERENCES

[1] Abhisek Pande,R C Tripathi,"A Survey on Wireless Sensor Networks Security" International Journal of Computer Applications ,Volume 3 – No.2, pp 43-49,June 2010.

[2] Yong Wang, Garhan Attebury , and Byrav Ramamurthy "A survey of security issues in Wireless sensor networks", volume 8, NO. 2 IEEE communications Surveys, pp 1-22, 2006.

[3] Daojing He, Student Member, IEEE, Chun Chen, Member, IEEE,Sammy Chan, Member, IEEE, and Jiajun Bu, Member, IEEE," DiCode: DoS-Resistant and

Distributed Code Dissemination in Wireless Sensor Networks", IEEE Transactions On Wireless Communications, Vol. 11, No. 5, May 2012

[4] Jaydip Sen "A survey on wireless sensor networks security" International Journal of Communication Networks and Information Security (IJCNIS) Vol. 1, No. 2, pp 189- 196, August 2009.

[5] 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.

[6] B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure SensorNetwork Routing: A Clean-Slate Approach," CoNEXT: Proc. ACM CoNEXT Conf., 2006.

[7] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", *Proc. MobiCom*, 2002

[8] S.H. Jokhio ,I.A. Jokhio, A.H. Kemp, "Node capture attack detection and defence in wireless sensor networks", IET Wirel. Sens. Syst., Vol. 2, Iss. 3, 2012

[9] H. Chan and A. Perrig, "Security and Privacy in SensorNetworks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

[10] Wenjun Gu, Neelanjana Dutta, Sriram Chellappan, and Xiaole Bai, "Providing End-to-End Secure Communications in Wireless Sensor Networks", IEEE Transactions On Network And Service Management, Vol. 8, No. 3, September 2011.

[11] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of Quality (RoQ) Attacks on Internet End-Systems," *Proc. IEEE INFOCOM*, 2005.

[12] R.Abirami , G.Premalatha ,"Depletion Of Vampire Attack in Medium Access Control Layer using Interior Gateway Routing Protocol ", IEEE, S.A COE,Chennai,pp1-5,2014.

[13] M.G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," Proc. First ACM Workshop Wireless Security (WiSE),2002.

[14] Sunil Bhutada,Kranthi Kumar,Manisha ,"A Novel Approach for Secure Routing Protocol: To Improve Life of Network", IEEE,pp 112-117, 2014.

[15] A.D. Wood, J. A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", Dept of Computer Sc., University of Virginia, 2002.

[16] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot, "Optimized Link State Routing Protocol for Ad-Hoc Networks", *Hipercom Project*, 2003.

[17] Taekyoung Kwon, Member, IEEE, and Jin Hong,"Secure and Efficient Broadcast Authentication in Wireless Sensor Networks",IEEE Transaction on Computers,VOL.59, No. 8, August 2010.

[18] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks," Proc. Int'l WorkshopSecurity Protocols, 1999.

[19] B. Karp and H. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in Proc. ACM International Conf. Mobile Comput. *Netw.*, Aug. 2000.

[20] R. N. Duche, N. P. Sarwade, "Sensor Node Failure Detection Based on Round Trip Delay and Paths in WSNs", *IEEE Sensors Journal, Vol. 14, No. 2*, February 2014.

[21] S. Goldberg, D. Xiao, E. Tromer, B. Barak, and J. Rexford, "Path-Quality Monitoring in the Presence of Adversaries," *Proc. ACM SIGMETRICS Int. Conf. Measurement and Modeling of Computer Systems*, 2008.

[22] S.-H. Fang, C.-C. Chuang, C. Wang, "Attack-Resistant Wireless Localization Using an Inclusive Disjunction Model", *IEEE Transactions On Communications, Vol. 60, No. 5*, May 2012.

[23] Mauro Conti, Member, IEEE, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei, Member, IEEE, "Distributed Detection of Clone Attacksin Wireless Sensor Networks", IEEE Transactions On Dependable And Secure Computing, Vol. 8, No. 5, September/October 2011.

Authors Profile

Ms. Shweta A Ghate received her Bachelor of Engineering in Information Technology from St.Vincent Palloti College Of Engineering & Technology, Rashtrasanth Tukdoji Maharaj Nagpur University, Nagpur, Maharashtra, India. Currently she is pursing Master of Engineering from Department of Information Technology, MIT College of Engineering of Pune University. Her research interest includes Preventing the Vampire Attacks in Wireless Sensor Network.

Dr.Prof. Vivek S. Deshpande, Dean of Research and Development, MIT College of Engineering, holds Bachelors and Master of Engineering in Electronics and Telecommunication from Pune University and PhD from Nagpur University, Maharashtra, India. Currently he is doing research in Wireless Sensor Network, Embedded System and High Performance Networks. He has got 16 patents published on his name. His 23 years of teaching and industry experience is an asset to the organization. Currently he is working as Associate Professor in Department of IT. His expertise in the field of Wireless Sensor Network and Distributed System helps in guidance to PG student.

 DOI:10.15693/ijaist/2015.v4i10.28-34

Dr. Prof. A. S. Hiwale received PhD in E&TC. He is working as Professor, Head of the Department in Department of Information Technology, MIT college of Engineering, Pune, India. He is having more than twenty five year experience. His research interest is Wireless, Digital Communication