Efficient Data Transmission Using Energy Efficient Clustering Scheme for Wireless Ad-Hoc Sensor Network

Savitha.M[1],Dr. R.Manavalan[2]

[1] *Research scholar, Department of Computer Science,* [2] *head of the department of Computer Applications*

[1,2] *K.S.Rangasamy College of Arts and Science, Tiruchengode, TamilNadu, India*

***Abstract*- Wireless Ad-hoc Sensor Network is characterized with low power, low computational capabilities and limited memory nodes. 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. The proposed model is evaluated on Ad hoc on demand Distance Vector routing protocol and also compared with PLGP in terms of the parameters such as Throughput, Packet Delivery Ratio and Packet Delay Time.**

***Keywords*: AODV, BS, PLGP, EECS, OTCL**

1. INTRODUCTION

Wireless Ad hoc Sensor Networks are formed by collection of autonomous nodes for communication via radio without any additional backbone infrastructure [1]. The routing process are designed for secure communication even though, these protocol are affected by some attacks. Due to distributed nature of these networks and their deployment in the remote areas, these networks are susceptible to several security threats that can adversely affect their function.

Vampire attacks disable the networks permanently by draining battery power of sensor nodes. It affects the properties of networks such relation state between the nodes, remoteness vectors between the nodes, resource and location based routing. WASN are particularly in vulnerable position due to Denial of Service (DoS) attacks, and great deals of researches have been done to enhance WASN survivability [3], [14]. Schemes so far proposed to prevent attacks only in the short-term availability of a network but not for long-term availability for Denial of Service attack in network.

In packet processing, adversaries are important to perform the energy consuming. A continuously recharging adversary can keep one node permanently disabled. However, recall that sending any packet automatically constitutes augmentation, allow few Vampires to attack various honest nodes [4], [13]. A single Vampire may attack every network node simultaneously; the continuous recharging does not help except Vampires are more resource constrained than honest nodes. Protocols such as SEAD, Ariadneare securely designed but do prevent the vampire attacks [5]. The overview of the proposed model is given in section 1.1

1.1 Overview of the proposed model

An overview of the proposed system is given in Fig. 1.The data transmission process of

both the PLGP and EECS are tested on Ad hoc On demand Distance Vector Routing Protocol for analysing their performance using parameters like Throughput, Packet delivery ratio and packet delay time.

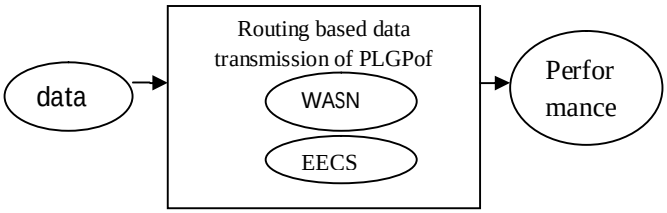


Fig.1 Block diagram of proposed system

In the rest of the paper, section 2 exposes a short review of related works regarding various attacks in Wireless Ad hoc Sensor Networks (WASN). Section 3 explains about the protocol that is used in the networks. The detailed explanation of PLGP and EECS are given in sections 4 and 5 respectively. Section 6 projects the experimental results and their discussion. The work is concluded in section 7 with future direction.

2. RELATED WORKS:

Kiran et al., Directed Graph (DG) establishment and Packet Transmission algorithm have performed to identify the packet dropping malicious nodes [6]. Haibin Sun et al., presented a distributed and efficient approach to dynamically detect and defend against low-rate TCP attacks in network [7]. Vahid Shah et al., presented the Distributed Maximum Lifetime Routing for Wireless Sensor Networks based on Regularization.

Regularization function is a strictly convex function, and a separable function. It is also used to vampire attack [8]. Mohammad et al., proposed a hierarchical architecture based intrusion detection system for wireless Ad hoc sensor network [9]. Reshmi et al., introduced the No-Backtracking property scheme to achieve high efficiency and secure authentication. The collection of identification technique is used to recognize the nearest neighbour node within the network [10]. Palle et al., presented an Optimal Energy Boost up Protocol (OEBP) and Energy Weighted Monitoring Algorithm (EMWA) to establish an optimal routing path [11]. PLGP does not offer a satisfactory solution during the topology discovery phase [2]. The detailed description of protocol and assumption used in the work is given in section 3.

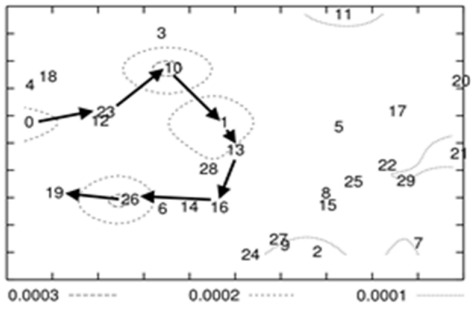
3. PROTOCOLS AND ASSUMPTIONS:

Generally two kinds of protocols are mainly considered for secure routing, such as On Demand Routing Protocols and Static Protocols [12], [15]. In on-demand routing protocol, the topology is discovered at the time of transmission of packets whereas in static routing protocol topology is discovered at the initial set up phase.

The battery power of the Nodes in sensor networks are limited [13] and a node will permanently disable from the network once its battery power has been exhausted. A single vampire has the ability to attack every node in the network. Hence, the continuous recharging of the node will prevent from vampire attacks and the attacks are more resource constraint than honest node [2], [24].Vampire attacks may affect different types of routing protocol. Two types of attacks such as Carousal attack and stretch attack have been discussed here under.

Carousel attack:

In this attack, an adversary sends a packet with a route which is composed as a series of loops to 0 to 19, such that the same node appears in the route many times that appears like cyclic. This strategy increases the length of the route beyond the number of nodes in the network. The limited numbers of allowed entries are composed by the source before the loop starts. The figure 2(a) and 2(b) shows honest scenario and carousal attack in the network.



2 (a) Honest scenario: node 0 sends a singlemessage to node 19

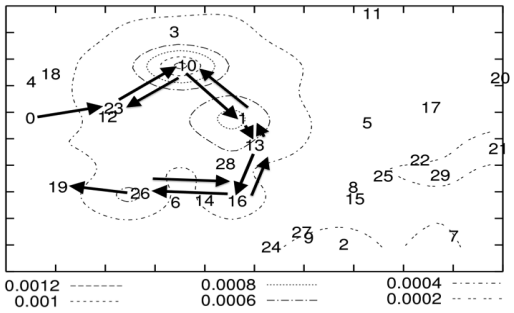


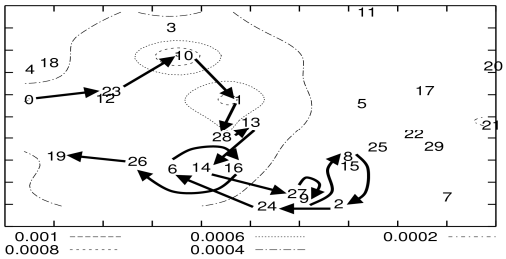
Fig 2(b) carousal attack(malicious node 0) the node traversed by the packet are the same as in (a)but the loop overall forwardingnodes roughly triples the root length(the packet traverse the loop more than once)

Fig: 2 carousel attack in WSN

Figure 2(a), the source node 0 transmits the message to the destination node 19 use the shortest optimal path in the topology. This is calling an honest scenario. In the second diagram, the node 0 transmits the message to the destination node 19 but the same time the source node becomes malicious and generates loops along the traversal path to increase the usage of energy in the network. There are various circular loops formed at node 10,1,16 and 26.It targets the limited verification of message headers at forwarding nodes, repeatedly traverse the same set of nodes.

Stretch attack

In this type of attack, the malicious node constructs paths to transmit the message to the destination node (which may be an honest one) which is far longer than the optimal path in the topology. An honest node select the path from source to destination, but the malicious node selects a longer route its affects all nodes in the network. It increases path length of the packet process by number of nodes along the shortest path between the adversary and packet destination. The figures 3 illustrated the stretch attack.



Stretch attack (mailcious node 0): the node diverts from the optimal path between source and destination,roughly doubling-up in length. note down that while the per node energy consumption increase is not as drastic as in (b), the region of increased energy consumption is large. Overall energy consumption is greater than in the carousel attack, but extend more evenly over more network nodes.

Figure: 3 Stretch attack in WSN

Comparing the diagram(c) with (a), the latter one is of an honest scenario where node 0 transmits a message to node 19 using the best optimal path available in the network topology. However in the diagram(c), the malicious node constructs artificial long paths starting from the node 28 where a diversion takes place to nodes 13, 14, 27, 9, 8, 15, 2, 24 and 6 using the longer optimal path. The energy usage of carousel attacks is higher compared to other attacks since in carousel attack, the nodes along the shortest path are affected.

3.1 AD HOC ON DEMAND DISTANCE VECTOR (AODV)

Ad hoc On-demand Distance Vector (AODV) routing protocol uses an on-demand approach for finding routes. In AODV, when a source node needs to send data, it initiates the route discovery process. The key feature of this protocol is distributed nature and the protocol has capable of both unicast and multicast routing. The route request packets use sequence numbers to ensure the

freshness of routes. It is loop free, self-sharing and scales to large numbers of mobile nodes. AODV uses only symmetric links because the route reply packet follows the reverse path of route request packet. AODV define three types of control messages for route maintenance: RREQ, RREP and RERR.

RREQ: a route request message is transmit by a route required node.

RREP: a route reply message is unicast reverse to the originator of a RREQ.

RERR: route error message is used to notify other nodes for the loss of the link.

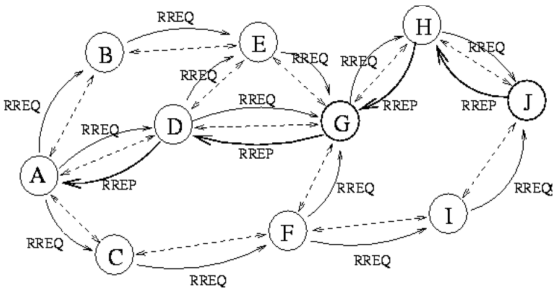


Fig 4: process of AODV protocol

The figure 4 illustrated an AODV routing process. Node A initiate the route for transmit a message. A transmit a RREQ message to all of its neighbours in the network. While this request is forward to J from it, J generates a RREP. This RREP is back unicast to A using the nodes H, G and D.

Routing table are maintained for update their information. A node once getting RREQ may send a route reply (RREP), if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. In this case, it unicast a RREP back to the source, else if broadcast the RREQ.

Once a source node stops the sending data packets, the link will time out and ultimately be deleted from the intermediate node routing table. If a link break occur while the route is active, the node propagates the route error message to the source. After receiving the RERR, the source node can reinitiate the route discovery process.

4. PLGP

PLGP is a clean-slate secure sensor network routing protocol developed by Parno, Luk, Gaustad and perrig. It is designed for security, is vulnerable to vampire attacks.PLGP consist of Topology discovery phase and Packet forwarding phase. Discovery process is most effective and it organizes nodes into a tree that will be used for addressing scheme. When discovery begins, nodes discover their neighbours using local broadcast and build a tree of neighbour relationships or group relationship that will be used for routing. At the end of the discovery, each node computes the same address to the other nodes in limited networks. In the tree, leaf nodes represented physical nodes and virtual addresses represented position of nodes. The figure 5 shows the PLGP tree structure.

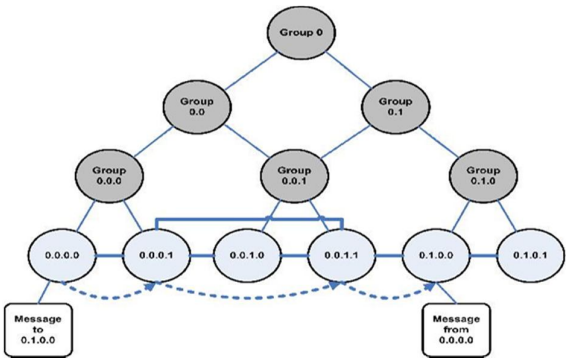


Fig 5: PLGP tree structure

Topology discovery: Discovery begins with a time limited period which every node must announce the presence of broadcasting certificate. Each node starts its own group of size, one with a virtual address 0. Every node stores the identity of 1or additional nodes through that it detected an announcement that another group exists. When two individual nodes form a group of size two, one of them takes the address 0 the other become 1.Each group will initially choose a group address 0; and will choose 0 or 1 when merging with another

group. Each group member prepends the group address to their own address. End of this topology discovery, each node learns every other nodes and it virtual address, public key and documentation.

Packet forwarding:During the packet forwarding, all decisions are made independently by each node. When a node receiving a packet, it determine the next hop by finding the most significant bit of its address that differs from the message originators address. The logical distance of the destination is computed in every forwarding by using node address. Figure 6 represent the packet forward function.

ParnoLuk Gaustad Perrig Routing Algorithm(PLGP) for packet forwarding

Input: No of sent data packets from source node.

Output: No of received data packets at the destination node.

Phase 1:[PLGP forward packet (p)]

1.1: Store the address of the source node (p) and the closet neighbour node of source node in the unique variables S and C.

1.2: If data packets decide C is very close neighbour node of it then forwards the data packet (p) from source to neighbour node.

Else

Choose next neighbour node (r) and forward data packet to r.

1.3: When B receives this packet, B adds the cost and its path information to the packet. This entire packet sends to C.

1.4: When C receives the packet, above process will repeat until the packet reach the destination (E).

Fig: 6 PLGP with packet forward function

Provable Security against vampire attack:

In PLGP, modification of the forwarding phase is used to avoid attacks. No backtracking property is introduced for packet traversing in the network. This property is satisfied for a given packet if and only if it consistently makes progress towards its destination.

PLGP does not satisfy no backtracking:

In PLGP, packet paths are constrained by physical neighbour relationships and the routing tree. In tree, two nodes have the same parent (if and only if) they are physical neighbours. So, the two neighbour nodes sharing an ancestor path to each other. Then every node can holds an identical copy of the address tree, every node can verify the next optimal next path. This is not sufficient for no-backtracking, since nodes cannot be traversed in the previous path. To preserve no backtracking, a verifiable path history is added to every PLGP packet similar to the route authentication. PLGP with attestations (PLGPa) uses the packet history together with PLGP'a tree structure to securely verify the progress with packet traverses by at least one honest node.

ParnoLukGaustadPerrigRouting Algorithm(PLGP)

Input: No of sent data packets from source node.

Output: No of received data packets at the destination node.

Phase 2:[PLGP secure forward packet p]

2.1: Store the attestation of source node in the variable a.

2.2: Drop the data packet (p) if it never contains signature and attestation of source node and also it is not a neighbour node o source node. Consider next node as a source node.

2.3: Find the neighbourhood nodes by checking the signatures and attestations and store them in a file p′.

2.4: Transmit the data packets towards the destination.

Fig: 7 PLGPa packet forward function

The figure 7 represented the secure forward packet function. Node n forwards packet p, by attaching non replayable attestation. These signatures form a chain and attached to every packet for validates its path. Every forwarding node verifies the attestation chain to ensure that the packet has never travelled away from its destination.

PLGPa satisfy no-backtracking:

Honest node can broadcast and receive messages in the network without overheard by any other node. These nodes can compose forward, allow or fall

messages and malicious nodes can also arbitrarily transform. An adversary controls m nodes with their corresponding identity certificates. Finally, the adversary cannot affect the connectivity between any two honest nodes. In PLGPa, all messages are signed by their originator; messages from honest nodes cannot be modified by malicious nodes. No backtracking scheme provides the guarantee of packet progress.

5.0 ENERGY EFFICIENT CLUSTERING SCHEME

The Energy Efficient Clustering Scheme (EECS) based routing algorithm for dynamic sizing of nodes in wireless sensor network. It provides equal distribution of energy in network to increase the lifetime. In EECS, the nodes are partitioned into a set of clusters. The communication made directly between the cluster head and base station. Each node can compute its appropriate distance for the BS based on the received signal strength. The node uses computed distance to select the proper power level when it communicates with the base station.

The main advantage of this algorithm is the full connectivity for longer duration and it provides reliable sensing capabilities for a longer period. It also produces the uniform distribution of cluster head.

The source node sends all data to all it's nearest neighbouring nodes. The energy efficient clustering scheme divides the data into a number of clusters and identifies the correct destination node to send the data in the network via proper routing path. The EECS scheme also improves the quality of service. The functionalities of Energy Efficient Distributed Clustering Algorithm are shown in Fig 5.

Energy Efficient Clustering Scheme (EECS)

Input: No of sent data packets from source node.

Output: No of received data packets at the destination node.

Step 1: The N number of nodes which have energy, source node, neighbourhood nodes and destination node.

Step 2: Partition the node into several clusters and choose one cluster head among them to
Send message for 1 hopat first.

Step 3: Do step 2 repeatedly if multihop are needed to transmit the message to destination.

Step 4: Cluster head check the state whether the destination has received the data or not.

Step 5: if destination receives data within single hop then stop the transmission otherwise
extend the transmission time for transmitting data through multi hop towards
destination node.

Step 6: Store the data packets that are received at the destination through single hop and
multi hop neighbourhood nodes.

Fig 8: Energy Efficient Clustering Scheme (EECS)

6. PERFORMANCE ANALYSIS

To analyse performance of the AODV by using path connected Networks. The replication surroundings are produced using NS-2, for a wireless sensor networks. NS-2 was using C++ language as well as it has used for OTCL. It came as addition of Tool Command Language (TCL). The execution approved out using a cluster environment of 19 wireless mobile nodes rootless over a simulation area of 1200 meters x 1200 meters level gap in service for 10 seconds of simulation time. The sources create multiple packets and sending to the destination node; each data has a steady size of 512 bytes.

Table 1.Simulation Setup

Parameter	Values
Version	Ns-allinone 2.28
Protocols	AODV
Simulation Area	1200m x 1200m
Broadcast Area	250 m
Transfer model	UDP,CBR
Data size	512 bytes

The simulation is conducted for finding the shortest path of the network model. The performance of the

proposed method is analysed using evaluation metrics such as throughput and end to end delay and packet delivery ratio. The short descriptions of these parameters are given here under.

Throughput is the amount of data transferred in a given period of time. A higher throughput indicates that the network performance is better while maximize the packet delivery ratio and minimize packet delay. Throughput is defined as

Throughput= R /T

where R means total number packets to be send; T is time taken for sending the packets

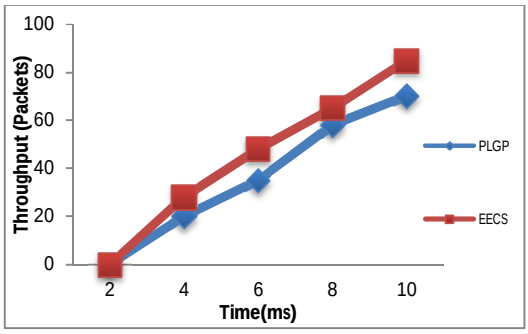


Fig: 9 Comparison of existing system and proposed system throughput

The throughput achieved by the methods PLGP and EECS for various times slot are provided in Table2. It clearly shows that the throughput of EECS is higher than PLGP with AODV for all time intervals. It is observed that for duration of 10 milliseconds the throughput of EECS is 79% where as throughput of PLGP technique is only 69%.

Table2. Throughput comparison table

Time (ms)	Throughput	
	PLGP	EECS
2	0	0
4	20	28
6	36	48
8	58	65
10	69	78

From the table, it is noted that EECS delivers packets 12% higher than the PLGP with AODV. It suggests that the EECS method can potentially improve the performance of the system.

The End to End Delay is computed from the packet delay during data transmission from node to node due to unexpected traffic congestion. It is calculate as $D = (T_r - T_s)$/ no of connections

where D is the end to end delay, T_r is receive Time and T_s is sent Time.

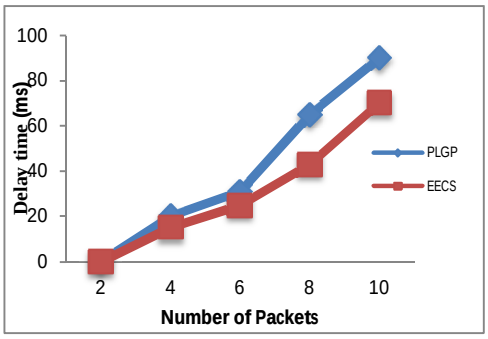


Fig: 11Comparison of packet delay time (ms) using PLGP and EECS methods

The graph 11 shows the end to end delay for data transfer from source to destination. End to end delay refer to the time taken for the packet to the transmitted across a network from source to destination. The PLGP method takes more delay time than EECS method. The delay time of these methods for number of packets transmitted over network is listed in Table 3. The numerical value in the Table shows that the delay time of EECS is considerably lower than PLGP. The delay time for sending 6 packets using PLGP method is about 30%time delay while EECS method achieves the same in 25%. Finally minimum end to end delay achieved by using EECS approach for data communication.

Table 3. Packet delay time (ms) using PLGP and EECS methods

Packets	Packet delay %	
	PLGP	EECS
2	0	0
4	20	15
6	30	25
8	58	43
10	87	76

The Packets Delivery Fraction (PDF) refers to the ratio of packets transmitted and received from the source to destination successfully over the network. The PDF ratio is measured in percentage as,

$$PDF = (\frac{P_r}{P_s}) * 100$$

where P_r is the received packets, P_s is the sent packets.

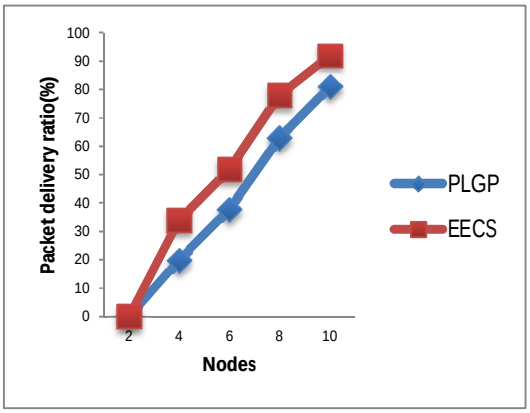


Fig 12. Comparison of Packet Delivery Fraction ratio of existing and proposed system

The fig 12 shows the value of PDR for data transfer from source to destination. PDR of 0.65 is achieved by using PLGP at the same time PDR of 0.78 is achieved by using EECS approach. Maximum PDR is achieved by using EECS.

Table4. Packet Delivery Fraction ratio (PDF) of PLGP and EECS methods

Time(ms)	PDF (%)	
	PLGP	EECS
2	0	0
4	23	34
6	41	52
8	65	78
10	83	92

The simulation study reveals that the proposed EECS method is superior to the existing method in terms of Throughput, End to end delay time and ratio of Packet delivery fraction.

7. CONCLUSION

In this paper, data transmission schemes such as PLGP and EECS are analysed on AODV routing protocol in Wireless Ad hoc Sensor Network (WASN) using NS2 simulator. PLGP protocol with no-backtracking property has performed to extend the lifetime of nodes. The Energy Efficient Clustering Scheme (EECS) with AODV routing algorithm is proposed for energy saving and increase the life time of the networks. Simulation results showed that the performance of EECS scheme is better for efficient data transmission from sender to receiver by updating the new shortest path and also resolving link break between source and destination. In future, researchers may concentrate on data transmission schemes to facilitate high throughput, high packet delivery ratio and minimum end to end delay in complex scenarios.

REFERENCE:

[1] Xiang Ji, HongyuanZha"Sensor Positioning in Wireless Ad-hoc SensorNetworks Using Multidimensional Scaling"In Proceedings of the 12th International Conference onComputer Communications and Networks, pp.527-532,2003

[2] Eugene Y. Vassermann and Nicholas Hopper "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks" IEEE Trans. Mobile Computing, vol. 12, no. 2, pp. 318-332 Feb-2013.

[3] T. Aura, "Dos-Resistant Authentication with Client Puzzles," Proc. Int'l Workshop Security Protocols, 2001.

[4]. L.M. Feeney, "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks,"

[5] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,"Proc. Fourth IEEE Workshop Mobile Computing Systems and Applications, 2003

[6] S.Sivanantham, K.Kirankumar, G.Saravanagokul," Identifying Malicious Nodes in Wireless Sensor Networks using Node Classification" International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 9, 2013

[7]Haibin Sun John C.S. Lui"Distributed Mechanism in Detecting and Defending against the Low-rate TCP Attack"International Conference of Network Protocols (ICNP) 2006, Berlin, Germany

[8] Vahid Shah-Mansouri and Vincent W.S. Wong" Distributed Maximum Lifetime Routing in Wireless Sensor Networks Based on Regularization"Proc. IEEE Transactions on, Ad-hoc and Sensor Networking Symposium, 2007

[9] Mohammad Saiful Islam Mamun" Hierarchical Design Based IntrusionDetectionsystem for Wireless Ad Hoc Sensor Network" International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010

[10] Vidya.MReshmi.S "Contending Against Energy Debilitating Attacks in Wireless Ad Hoc Sensor Networks" International Journal of Innovative Research in Advanced Engineering (IJIRAE) Volume 1, Issue 1 2014
[11] Monica Palle, SeelamSaiSatyanarayana Reddy "Detection Elimination and Overcoming of Vampire Attacks in Wireless Ad hoc Networks " IJRIT International Journal of Research in Information Technology, Volume 2, Issue 6, 2014, Pg: 224-237
[12] Gergely A´ cs, LeventeButtya´n, and Istva´nVajda "Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks" IEEE journal March 2010 [7] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.
[13] Ray-Guang Cheng, Shin-Ming Cheng, and Phone Lin, "Power-Efficient Routing Mechanism for ODMA Systems" IEEE transactions on vehicular technology, vol. 55, no. 4, July 2006
[14] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, Effects of denial-of-sleep attacks on wireless sensor network MAC protocols, IEEE Transactions on Vehicular Technology 58 (2009), no. 1.
[15] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.
[16] A.J. Goldsmith and S.B. Wicker, "Design Challenges for Energy-Constrained Ad Hoc Wireless Networks," IEEE Wireless Comm., vol. 9, no. 4, pp. 8-27, Aug. 2002.
[17] Shalini Jain, Dr.Satbir Jain, "Detection and prevention of wormhole attack in mobile adhoc networks", vol. Jan 5, 2010.
[18] SoramRakesh Singh, NarendraBabu C R " improving the performance of energy attack
detection in wireless sensor network by secure forwarding mechanism " International Journal of Scientific and Research Publications, Volume 4, Issue 7, 2014
[19] Monica Palle, SeelamSaiSatyanarayana Reddy "Detection Elimination and Overcoming of Vampire Attacks in Wireless Ad hoc Networks " IJRIT International Journal of Research in Information Technology, Volume 2, Issue 6, 2014, Pg: 224-237
[20] SoramRakesh Singh, NarendraBabu C R " improving the performance of energy attack detection in wireless sensor network by secure forwarding mechanism " International Journal of Scientific and Research Publications, Volume 4, Issue 7, 2014
[21]S.BlessyVedhaP.Petchimuthu "A Captivating Approach for Disclosing Vampire Intrusion in WSN" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 3, 2014
[22] Jose Anand, K. Sivachanda "Vampire Attack Detection in Wireless Sensor Network" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 4, 2014

AUTHOR'S BIOGRAPHY

M.Savitha received her M.Sc (Computer Science) degree from Vivekananda Arts and Science College, tiruchengode Affiliated to periyar University, salem in 2010.she is pursuing his M.Phil (Computer Science) degree Under the Supervision of Dr.R.Manavalan. His Area of interest is Mobile Computing.

Dr. R. Manavalan is working as an Associate professor and Head in the Department of Computer Applications. He obtained his PhD in Computer Science from Periyar University and published numerous research Papers in International Journals and also presented papers in various National and International Conferences. His Areas of interest are Soft Computing, Image Processing andAnalysis, Theory of Computation, Intelligent Computing and Mobile Computing.