A SURVEY ON PROTECTED STEERING FROM BEGINNING TO END TRUST NODES IN WSN

Dr. A. SINGARAVELAN

Vice Principal
SVA College of Polytechnic, Namakkal, Tamilnadu, India

***Abstract*: Wireless Sensor Networks (WSN) are the upcoming and demanding knowledge with low dispensation and battery power. Security becomes a major issue in WSN. Because it is wireless in nature and prone to various types of attacks and losing of data packet. The major issue in WSN is security. The secure routing is the technique which is highly supporting for avoiding the above issues. In this proposed paper various security mechanisms are discussed to find malevolent nodes and to do protected routing. Our main motto is to find the trust node by using trust model and the malicious report is checked. Breadth First Search is used for routing. It provides the security features with minimum overhead and energy efficiency.**

***Keywords*: WSN, Breadth First Search, Secure Routing, Software Agents.**

I. INTRODUCTION

WSN are collection of nodes where each node has its own sensor, processor, Transmitter and receiver. The sensors are low cost devices that perform a specific type of sensing event. Being of low cost such sensors are deployed densely throughout the area to monitor specific event [2]. WSN are highly distributed networks of small lightweight wireless nodes. Sensor nodes are called as mote. It monitors the environment or system by measuring physical parameters such as temperature, pressure, humidity etc. Sensor networks are widely applied in various filed such as environment monitoring, military applications, health care and home intelligence. The major issue in WSN is security requirements. One of the main issues is secure routing [8]. Because of the wireless nature routing has to be done in secure way to avoid the information loss, and various attacks. The existing systems are available for trust node identification and secure routing are discussed in Table1. It discuss with the different techniques to identify the malicious node, and energy efficiency, overhead and security features. That works didn't completely provide security features, energy efficient, less overhead. And also they dint deals with routing scheme. The proposed work is provided to overcome the security challenges and do routing in a secure and efficient way. In this we use trust based system along with shared key with the help of agent technology to find the trusted node and malicious node is checked whether it is true or not and route it using BFS.

The section II depicts about the wireless sensor network, its security challenges, Agent technology and BFS. Section III discuss the existing algorithm, section IV comprises the proposed work. Section V comprises the conclusion.

II. BACKDROP TRECHNOLOGY

This section deals with the background techniques related to write this paper. That is WSN, secure routing, challenges, Agent technology and BFS.

A. Wireless Sensor Networks (WSN)

WSN consists of sensors that are randomly distributed in an ad hoc manner. The sensor nodes sense some physical phenomenon and then the gathered information is processed. Although deployed in an ad hoc manner it needed to be selforganised and self-healing. WSN provides a bridge between physical and virtual worlds. Sensor have limited sensing region, processing power and energy. Each node of the sensor network consists of four subsystem: sensor subsystem senses the environment, the processing subsystem performs computations on the sensed data, and the communication subsystem is responsible for message exchange with neighbor sensor nodes and power unit. Sensor network are designed based on low node cost, low power consumption, self-configurability, scalability, adaptability, reliability, fault tolerant, QOS, support and security.

Energy efficiency is more important in sensor network to ensure network performance and prolong network lifetime. The main reason for waste of energy are ideal listening, collision, overhearing, control overhead and over matting, in medium access unlike MAC protocols, WSN schemes must allow sleep modes during radio inactivity to maximize energy efficiency. Two main classes of protocols are contention based and contention free. Routing in wireless sensor network can be made robust and efficiency by incorporating different types of local information such as link quality, link distance, residual energy and position information. Overhead includes the processing time, storage, memory consumption for a process.

B. Issues in WSN

Wireless sensor networks are vulnerable to security attacks due to the broadcast nature of the wireless transmission medium. The attacks are broadly classified in two categories as active and passive attacks [3]. The monitoring and listening of communication channel by unauthorised attackers are known as passive attacks. Some of the attacks are, monitor and eavesdropping, traffic analysis. The unauthorized attackers monitors, listens and modify the data in channel are known as active

attacks. The active attacks are attacks on information in transit, selective forwarding, black hole and sink hole, hello flood attacks and denial of services. These attacks are the significance of malicious nodes in wireless networks.

Monitor and eavesdropping:- Eavesdropping is secretly listening to the private conversation. The eaves dropping attack is a serious security threat to WSN. In this malicious node detect the information by listening to the message transmission in the wireless medium. And also malicious node steals the information by sending queries to transmitters by disguising themselves as friendly nodes. This attack is also known as confidentiality attack.

Selective forwarding: - A malicious node can selectively drop only some packets. This dropping of node increases when it is combined with sink hole or acknowledgement spoofing. The attack can be used to make a denial of service attack targeted to a particular node. In this the malicious node will behave as a black hole and refuses to forward the packet [6].

Hello Flood: - In this attack a malicious node can send record or replay messages with high transmission power. Many protocols HELLO message are needed to route discovery, the nodes receiving that packet assume that the node is in its radio range of the sensor [6]. It creates an illusion of being a neighbour to many nodes in the networks and confuses the network routing. It attack mainly on protocol that require sharing of information for topology maintenance or flow control.

Sybil Attack: - The Sybil attack is targeted to undermine the distributed solutions that rely on multiple nodes cooperation or multiple routes. In a Sybil attack, the malicious node gathers several identities for posing as a group of many nodes instead of one. This attack is not relevant as a routing attack only. It can be used against any crypto-schemes that divide the trust between multiple parties. Sybil attack can reduce the effectiveness of fault tolerant schemes [6].

Sinkhole (Black hole):- A malicious node uses the faults in a routing protocol to attract much traffic from a particular area, thus creating a sinkhole. Tricking users advertising a high quality link. Use a laptop class node to make the good route as a faulty one. Highly attractive and susceptibility due to communication pattern. Geo-routing protocols are resistant to this attack [5].

Wormholes: - This attack needs two malicious nodes. This main aim is to distort routing with the use of low latency out of bound channel to another part of the network where messages are replayed. This attack is more commonly involve where the two distant malicious node collide with each other [6]. It is difficult to detect when it is conjunction in Sybil attack.

C. Challenges

Wireless medium is less secure because its broad cast nature makes eavesdropping simple. Wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Ad-hoc nature of sensor networks means no structure can be statically defines. Nodes may fail or be replace the network must support self configuration. Sensor nodes are deployed in hostile environment; it faces the possibility of destruction or capture by the attackers. Providing security in WSN is even more difficult in MANETS due to the resource limitation of sensor nodes and security concerns remains a serious impediment to widespread adaptation of these WSNs [5]. The highly hostile environment represents serious challenges for security researches. Secure model should use battery life efficiently. WSN goals [4] include confidentiality, Integrity, Data origin authentication, Access control, Availability. It has to design against the attack such as eavesdropping, fabrication, injection, modification, node capturing [7]. The main research areas for security in WSN [8] include key management, secure location, secure routing, attacks and preventions.

D. Secure Routing

Routing is one thing that distinguishes WSN from MANET and other networks. Routing is a challenging task in WSN because more number of sensor nodes is deployed in ad monitoring area. Because of wireless nature the WSN prone to various types of security issues, routing is one main area have to focus. Secure routing has to be done to avoid signal spoofing, injection of fabricated message into the network, alteration of messages while transmission, avoid formation of loops, avoid redirection of shortest path. System fault, error data may also cause the network failure. To overcome the attacks and information loss, secure routing has to be done [20]. Secure routing through the trusted node is one of the ways to avoid the attacks mentioned above. Secure routing protocol have to consider the sensor network limitation such as limited memory, energy, resource constrained.

E. Trusted Node

Trust has to establish between nodes to ensure the trustworthiness of the node. Trusted node refers to the node which behaves normally, that is sensing and forwarding packets to proper destination without any information loss. Many types of schemes are used to find the trust node and detection of malicious node, some of them are discussed here. In Trust based method, Trust values can be calculated from the reputation and behaviour of the node. The system is given with the threshold above the threshold the node is normal node otherwise it is malicious. In cryptography key exchange mechanism used to find malicious nodes.

F. Agent Technology

Software agent is a persistent, goal oriented computer program that reacts to its environment and runs without continuous direct supervision to perform some function for an end user or another program. The agents offer effectiveness, efficiency, transparency and optimization. The agents are mobile and static. Mobile agents move from system to another and do their execution, features include autonomy, learning. Static agents are static in nature, it do the same work as mobile agents other than mobility.

G. Breadth First Search (BFS)

BFS is a graph search algorithm that begins at the root node and explores all the neighbours' node. Then for each those neighbour node it explores their unexplored neighbour nodes, and so on until it finds the goal. If there is more than one path then BFS can find the shortest path. The BFS algorithm is given below:

1. Visits all the vertices and edges of a Graph
2. Determines whether Graph is connected
3. Computes the connected components of Graph
4. Computes a spanning forest of Graph

III. SECURITY SCHEMES IN WSN

In this section, different types of algorithm and architecture are available to find the trusted node and to find the secure routes are discussed.

Algorithm 1: An Authentication scheme for locating compromised nodes in WSNs In this paper they propose a COOL protocol [9], to identify the misbehaving nodes. The well behaved nodes are identified by set of incoming and outgoing messages. Each message is signed by using incremental hash function. In this work (ADHASH) [10] hash function is used for authentication. The sink verifies the hash value of the node matches or not. By using the hash values we compare the node and link consistency. The malicious node id found it is removed and the link is found not reliable both nodes are removed. In this we first initialise the unique id to each node and the key by using hash function, next we perform route discovery by using HELLO messages next we check the secret key of each node and it is routed along the discovered path. Each node has the hash value of each links, the hash values are collected by the sink. Incoming and outgoing hash value of each node is checked, by this we find compromised node. The incoming and outgoing hash values of each link are checked by this we find inconsistent link. The id of the suspicious node is sending to cluster head it replaces the new node. It discriminate the false report, locate compromised node, Injection attacks and report dropping at relay can be identified, has small overhead. If the sub region is isolated without cluster head, sink cannot decide the status of the node. Nodes may be excluded because of signal blocking and collision.

Algorithm 2: TARF - A Trust Aware Routing Framework for Wireless Sensor Networks In the paper [10], they are discussing a framework for trust aware routing. It incorporates trust manager and energy watcher to make routing decision. We identify the trustworthiness of a node using trust manager and calculate the energy cost by using energy watcher. Energy watcher is responsible for calculating the energy cost based on average energy cost of successfully delivering a unit sized data packet from N to base station. Energy watchers on the node monitors the energy consumption of one hop transmission to its neighbours and process the processes the energy cost report from neighbour to maintain the energy cost in entire in neighbourhood table. Trust manger keep track of network loop and broadcast the message consists of undelivered data to maintain trust level. To detect the loop it uses the source id and forward sequence interval. If the loop id detected by N for few times the trust level of next hop node is low. To detect the traffic misdirection it compares the source id and forward sequence interval that is recorded in fast few periods about undelivered data. It computes the delivery ratio with respect to number of successfully delivered packet to the number of packet forwarded. By using this information we can route the data securely with effective energy. It has efficient use of energy, higher throughput achieved in traffic misdirection. It is applicable to medium sized network, Specific protocol have to be built over TARF to achieve latency, load balance and fairness.

Algorithm 3: A Recent Technique to Detect Sink
Hole Attacks in WSN

They are proposed a scheme to defend against sink hole attack using mobile agents. It proposes two algorithms, that is Agent navigation algorithm and data routing algorithm, every agent has its own brief case that contains the distance between nodes and counter contains the information about particular node as the one hop neighbour. Each node has a counter that contains the number of times the node visited the node. Agent navigation algorithm, in this each node maintains a cache, the agents updates the information in the cache from its brief case. The agent gives the current node information and decides the next destination node. In this, the mobile agent visits every node and gives network information. Data routing algorithm uses the network information to route packets. The mobile agent gets the information matrix table it contains the link available between the nodes. By this the data are routed through the most repeated and less weight path. False path is avoided, Encryption and decryption process is avoided, does not require more energy. Overhead increases for larger network

Algorithm 4: Providing Trust in Wireless Sensor

Network using a Bio-inspired Technique. they propose a bio-inspired trust and reputation model, based on ant colony system. They select the most trustworthy node through the most reputable path. The client sends the ants equal to number of senor nodes that finds the server and return to the client, it stores the pheromone traces. Every node has the trace of its neighbour. By using the most reputable path we can find the trustworthy node in that path. It is accurate and reliable, offers punishment and reward. It does not distinguish benevolent and fraudulent based on a certain service. Collusion formed when malicious servers is more than 90%.

Algorithm 5: UNMASK: utilizing Neighbour

Monitoring For Attack Mitigation in Multi hop Wireless Sensor Networks they propose a framework for detecting diagnosing and isolating malicious nodes in network. For this they developed unmask and LSR (lightweight secure routing). UNMASK detects the malicious node and isolate away from the network to avoid future attacks by that node. In unmask, first we find the neighbour discovery by using HELLO message and that message attach the commitment key. In this stage every node has the neighbour list and their key. In this the one hop authentication is done by using this commitment string. Every node maintains a buffer, has a counter, the counter value increases when the node detects any delay or drop in the packet, and the messages are modified as considered as malicious node. Local response and isolation is done to propagate the malicious node information to its neighbour. In LSR it perform the on demand routing, combined with UNMASK it detect and isolate the node causing various attacks. For this it performs the Route discovery and Maintenance. In this they use the commitment key. Increases the number of node disjoint routes between a source and destination. It is against wormhole, Sybil, rushing, acknowledgement and ID spoofing attack. Neighbour discovery protocol cannot be secure for mobile networks.

Algorithm 6: A Direct Trust Dependent Link

State Routing Protocol Using Route Trust for WSNs (DTLSRP) In this paper they propose a trust dependent link state routing protocol by which we can determine the trusted node and route with the trusted node to eliminate the routing attacks. This work consists of five phases. In first phase we are calculating the node trust by using direct observation as successful packet transmission rate, latency. By this we rate the node trust value. In second phase they find the benevolent node that is whose trust

value is above certain threshold (0.5) considered as benevolent node. In third phase we find the path using link state routing protocol that is the path where the benevolent node is present. In fourth phase we calculate the route trust of the discovered path by using the trust value of each node in that routing path. Route trust values are calculated by multiplying the trust vale of all nodes in that path. In fifth phase, the route trust values are compared we can select the route where the route trust value is higher. Therefore the efficient route for data packet transmission is found, by founding the appropriate path we eliminate the routing attacks. Dijsktra's algorithms are not needed to find the shortest path, it is easily found and Overhead decreases. Trust value is based on direct communication to the node only.

Algorithm 7: A Novel Heuristic Approach based

Trust Worthy Architecture for Wireless Sensor Networks they propose HATWA the trust based architecture for WSN. In this the trust value is calculated by two methods that is trust is calculated in each node and it is calculated as a group or cluster. In this proposed work they have a monitoring node outside the network for storing the past interaction and history of the node. In node trust calculation, the trust value can be calculated by the information stored in network monitoring node. At group trust calculation, the monitoring node evaluate the trust of every node in the group, if 80% of the node are trusted in the group then the group is considered as trusted. The networking monitoring node architecture consists of three algorithmic model as security, mobility and reliability model. The architecture has 4 stages. In stage 1, trust can be based on fault tolerant mechanism, and stage 2 is for selection of secure routing protocol, stage 3 is for mobility and stage 4 deals with energy consumption. The initial trust value can be calculated by the direct observation and recommendation from the neighbours. This given as the input to the HATWA. In security model trust value is evaluated based on the access control, security routing and encryption. In mobility model, the trust vale of the mobility node based on the energy consumption of the node. In reliability model trust value is calculated by delay, latency, energy consumption. The outcome of the architecture gives the overall trust as the output. Offers less communication overhead, less energy consumption and memory. Mobility may affect the trust calculation.

Algorithm 8: Neighbour Based Malicious Node

Detection in Wireless Sensor Networks they propose neighbour based malicious node detection scheme, in this they consider event and periodic modes of operation, due to transient fault may mislead the network that results in wastage of energy and incorrect decision sometimes the normal nodes are removed. This method has two methods to find accurate malicious node as Data smoothing, variation test and confidence level evaluation. In data smoothing and variation test we have range, filter and variation test, the range block and variation test have same input, range bloc checks the input array whether it is in normal range or not. Variation test determines the difference in input in presence of vent detection and in no event detection. Filter performs the smoothing reading with the threshold value. In confidence level evaluation the initial value 1 or 0 is assigned to node based on the neighbour node decision. It represent the trust worthiness of node, each node updates its confidence node level and its neighbour node during event and periodic detection. This method accurately detects and isolates the malicious node which behaves normally. Accurate malicious node isolation, It has low false rate. Malicious node detection rate and misdetection rate should be maintained in faults and events.

Algorithm 9: Trust and Energy Aware Routing

Protocol Wireless Sensor Network they propose a trust and energy aware, it is a location based protocol for WSN. The trust values are calculated by the ATMP, in addition to that we adding location and energy to find the trustworthy path. This method consists of two phases, setup phase and forwarding phase. In setup phase each node calculates it cost value based on the trust values, energy level of the neighbor node, and location based on the distance between the node to the neighbour node, and the node to the base station. Such as the next best hop node is selected based on the trust value, energy level and location information. If the cost value is low, that node is chosen to send the packets. In forwarding phase the node forwards the packet depends on its trustworthiness of packets, it is determined by the trust value of source node, trust limit and MAC. It has Load balancing capacity. Energy efficient. Setup phase is done often, when the network size increases.

IV. PROPOSED WORK

The comparative study is done based on the basic requirement as Energy efficiency, overhead, and security features include verification, data privacy and integrity. Energy efficiency is the goal is achieved with minimum energy, overhead is due to memory, calculation time. By the comparative study, the various methods or architecture for malicious node detection are found. The different techniques are cryptography, ant colony system, trust and reputation. Cryptography is the method of encrypting the message using key, it can be decrypted only the key is know. The Ant Colony System algorithm is inspired by the behaviour of ants, specifically the pheromone communication between ants regarding a good path between the colony (server) and a food source (client) in an environment. Trust and reputation, trust value is based on the reputation and behavior of the node. From the survey, we identified that, the system which offers energy efficiency, less overhead and security features are considered as best scheme to route the data packet securely. The existing works as shown in Table 1 discuss some of the methods to find the trusted node and secure routing. In the existing works dint fully achieve the security goals, with minimum energy and overhead. And also it does not provide the option for checking whether the reported malicious node is true or not. With this concern, the new algorithm is proposed. The proposed work consists of trust model consists of probability model, MAC model, EAACK based Misbehavior node verification, and routing through the trusted node. Working of proposed work include (i) identification of trusted node and (ii) Routing through the node. Identification of Trusted Node

1. We can find the trust node based on probability model and MAC (Message Authentication Code) model. Probability model gives trust value based on behavior of node. In MAC model the verification of MAC is done.
2. If the MAC does not match, it goes to secure Acknowledgement mode. The report is sent to source and verifies the reported node by using misbehaving report phase. Routing through the node 1. Once the trusted node is found the BFS algorithm is implemented in this. The working procedure is of the proposed work is explained below

Step1:

i. Select the Probability model:
ii. .Assume an threshold value as 0.5,
iii. The nodes are given a rating based on the nodes behaviour.
iv. If rating above 0.5, considered as trusted node
v. Otherwise it is un trusted.

Step2:

i. Select the MAC model
ii. In this the message are encrypted by using the key, and it is send to the trusted nodes. The message is recomputed and MAC is checked. Mobile agents are responsible for carrying the encrypted message to check the MAC verification.
iii. If it is matches considered as trusted node and send Ack to the source.
iv. Otherwise move to step3

Step3:

i. Secure Acknowledgement (ACK) phase
ii. In secure acknowledgement (S-ACK) phase three nodes work together to find the malicious node, the node R4 sends S-ACK data packet (pkt1) to R5, then R5 forwards this packet to i6.the node R6 receives the pkt1 it has to send the S-ACK packet to R4.
iii. If R4 does not receive this acknowledgement, then the node R4 is considered to be malicious. It is reported to the source node.
iv. The source node switches to the Misbehavior Report Authentication (MRA) mode to ensure that the node is malicious or not.

Step4:

i. Misbehavior (malicious) report phase
ii. In MRA mode, it checks whether the reported malicious node is true or not.
iii. It checks whether the missing packet is reached the destination through any other node. When the destination node receives the MRA packet, it checks its local knowledgebase.
iv. If the missed packet is already received by destination node through different path. It is concluded that it is a false misbehavior report. That is R4 is considered as a malicious node is not true, who generated the report that is R6 is considered as malicious node.
v. Otherwise the misbehavior report is considered as true.

The static agents and mobile agents are implanted in each node static agents triggers the mobile agent to collect the information about the trusted node and malicious node and its path towards the destination. It maintains the list of trusted and malicious node that is identified by the proposed method. In this we use BFS for routing.

Let us consider a scenario shown in figure 1.

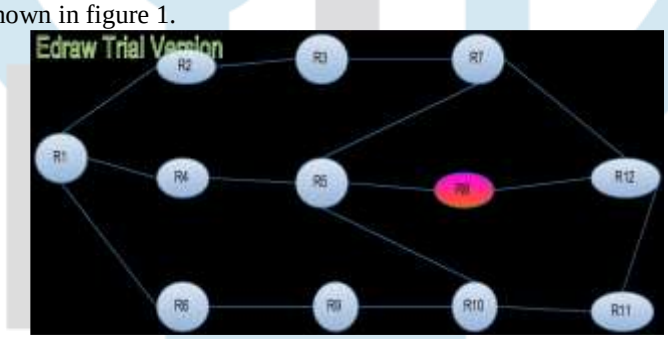

Figure1: Example of a scenario

In this topology (Figure1), R1 is source, R12 is destination, in this the available path to destination are as follows found by using BFS.

- R1-R4-R5-R6-R12,
- R1-R2-R3-R7-R12,
- R6-R12,

In this let us consider that the node R6 is malicious by the given algorithm. Suppose the route selected is R1-R4-R5-R6-R12. The mobile agent in R4 has to report the next node the path has a malicious node, so redirect the path through R7 or R8. It chooses the R7, because it is the shortest path to reach the destination. Thus the routing is done through the trusted node.

The proposed work is energy efficient, offers minimum routing overhead because we use agents to provide communication. It can improve packet delivery ratio, minimum packet latency and also we can achieve authentication, data confidentiality and integrity in WSNs and Provides high level of security.

V. CONCLUSION

In wireless sensor network, the security issues are the major concern. In the security issues secure routing is one main concept to achieve security in WSN. In this paper we discussed various existing methods to find the trusted node and secure routing. From all the work we conclude that, most of the work does not provide high level of security, and secure routing with energy efficient and reduced overhead. So in our proposed work we took this as a major concern and we designed an agent based

secure routing using trustworthy nodes. We have to simulate it by using NS2. Our future work includes implementing this system in real time and in a dynamic system.

REFERENCES

[1] D. Latha and K. Palanivel, "Secure Routing Through Trusted Nodes in Wireless Sensor Networks – A Survey", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)

[2] Volume 3 Issue 11, November 2014

[3] Pandey, A. and Tripathi, R. (2010). A Survey on Wireless Sensor Networks Security. International Journal of Computer Applications, 3(2), pp.43-49.

[4] M. Praveen Kumar, S. P. Santhoshkumar, S. Karthick ,"A SURVEY ON INTERNET OF THINGS USING WIRLESS SENSOR NETWORKS", INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH & DEVELOPMENT(IJSRD), Volume 5, Issue 11, Pages 500-506.

[5] Li, Zhijun, and Guang Gong. "A survey on security in wireless sensor networks." Department of Electrical and Computer Engineering, University of Waterloo, Canada (2011): 2008-20.

[6] V. Kumar, A. Jain, and B. P N, "Wireless Sensor Networks Security Issues, Challenges and Solutions," Int. Res. Publ. House, vol. 4, no. 8, pp. 859–868, 2014.

[7] Kavitha, T., & Sridharan, D. (2010). Security vulnerabilities in wireless sensor networks: A survey. Journal of Information Assurance and Security, 5, 31–44.

[8] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1, 293–315.

[9] Momani, M. and Challa, S. (2010). Survey of Trust Models in Different Network Domains. IJASUC, 1(3), pp.1-19.

[10] Bin, T.,Xian,Y.Y., Dong, L.,Qi, L.,&Xin,Y. (2010).A security framework for wireless sensor networks. The Journal of China Universities of Posts and Telecommunications, 17, 118–122.

[11] Zhang,Y.,Yang, J.,Li,W.,Wang, L.,&Jin, L. (2010).An authentication scheme for locating compromised sensor nodes in WSNs. Journal of Network and Computer Applications, 33, 50–62.

[12] Bellare M, Micciancio D. A new paradigm for collision-free hashing: incrementality at reduced cost. In: Eurocrypt'97, Lecture notes in computer science, vol. 1233, 1997.

[13] Zhan, G., Shi, W., & Deng, J. ((2010). TARF: A Trust-aware routing framework for wireless sensor networks. In European Conference on Wireless Sensor Networks (EWSN) (pp. 65–80).

[14] Sheela, D., Nirmala S., Nath, S., & Mahadevan, G. (2011, July). A Recent technique to detect sink hole attacks in WSN. White paper, Anna University.