ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Energy preservation in Wireless Sensor Networks through the Recognition of Trusted Node

Pratishtha Gupta

Research Scholar, Dept. of C.S., Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India

ABSTRACT: Remote Sensor Network (WSN) is the rising and testing innovation with low preparing and battery power. Security turns into a noteworthy issue in WSN; in view of its remote nature it is inclined to different sorts of assaults and losing of information bundle. Secure steering is vital to evade this kind of issues. They are numerous systems are accessible to give secure directing to WSN. In the proposed work, our fundamental point is to locate the trusted hub and steering is done through the hub to give secure directing. The trusted hub is recognized by utilizing QOS measurements and it is appraised. Furthermore allowing the untrusted hub to transfer demonstrates its character. It gives the security highlights least overhead and vitality proficiency.

KEYWORDS: Wireless Sensor Networks, Secure Routing, QOS

I. INTRODUCTION

Wireless Sensor Networks (WSN) is spatially distributed autonomous sensors to monitor physical and environmental conditions such as temperature pressure etc. 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 [1]. Sensor node consists of battery, microcontroller, transreceiver, external memory, sensors. There are two main applications are monitoring and tracking. WSNs are mainly used in military applications, health monitoring, fire detections etc.

Sensor networks are mostly deployed in public and uncontrolled area, therefore the security becomes a major issues. Security becomes a major concern in sensor network because of its broad cast nature. The main security goals in sensor network such as confidentiality, integrity, authentication, availability [2].

The major constrain in sensor network are energy, memory, transmission range fault tolerance, self organization and scalability [4]. The attacks are broadly classified in two categories as active and passive attacks [2]. These attacks are the significance of malicious nodes in wireless networks. The attacks include, Monitor and eavesdropping, Selective forwarding, Hello Flood, Sybil Attack, Sinkhole (Black hole), Wormholes [5].

The highly hostile environment represents serious challenges for security researches. Secure model should use battery life efficiently. It has to design against the attack such as eavesdropping, fabrication, injection, modification, node capturing [6]. The main research areas for security in WSN [7] include key management, secure location, secure routing, attacks and preventions. Secure routing is one of the ways to avoid this type of attacks. 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 [4]. Secure routing protocol should be designed to satisfy the energy and memory consumption.

In the proposed work, our main aim is to find the trusted node and routing is done through the identified trusted node to provide secure routing. And also giving the opportunity to an untrusted node to prove its originality whether it is really malicious or not. The trusted node is identified by using MAC model and it is rated. It provides the security features with minimum overhead and energy efficiency.

The rest of the paper as follows, Section 2 comprises literature survey, sections 3 discuss the proposed method, section 4 deals with the Simulation and Analysis, section 5 comprises of conclusion.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

II. LITERATURE SURVEY

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

In this paper [8] they propose a COOL protocol, to identify the misbehaving nodes. The well behaved nodes are identified by set of incoming and outgoing messages. Each message is signed by (ADHASH)[9] 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 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. It has efficient use of energy, higher throughput achieved in traffic misdirection.

In the paper [11] 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. Agent navigation algorithm, in this each node maintains a cache, the agents updates the information in the cache from its brief case. False path is avoided, Encryption and decryption process is avoided, does not require more energy. Overhead increases for larger network in this paper [12] 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.

In this paper [13] 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.. 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. Increases the number of node disjoint routes between a source and destination Neighbour discovery protocol cannot be secure for mobile networks

In this paper [14] 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 in third phase we find the path having benevolent node using link state routing protocol. In fourth phase we calculate the route trust of the discovered path by using the trust value of each node in that routing path. 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.

In this paper [15] they propose HATWA the trust based architecture for WSN. 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 evaluates the trust of every node in the group.

In this paper [16] 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. It has low false rate.

In this paper [17] they propose a trust and energy aware, it is a location based protocol for WSN. The trust values are calculated by the ATMP [18], in addition to that we adding location and energy to find the trustworthy path. This method consists of two phases. In setup phase each node calculates it cost value based on the trust values, energy level of the neighbour 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. It has Load balancing capacity. Energy efficient Setup phase is done, when the network size increases.

In this paper [20] ASERT, Agents effectively perform the function of finding trusted neighbours

Using probability based trust model and MAC model ensuring higher security and hence the secured routes are established. It consists of safeguard agency and routing agency. In the first phase, that is probability model agents visit all the neighbours and bring probability of all the neighbours using computational behaviour and in the second phase,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

agents ensure the trusted neighbours using MAC model. Routing agency establishes routes through the trustworthy neighbour's identified by safeguard agency.

In this the various methods or architecture for malicious node detection are found [3]. The different techniques are cryptography, ant colony system, trust and reputation. 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. 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.

III. PROPOSED SYSTEM

The primary security threat to MANETs routing is the possibility of an adversary disrupting traffic by compromising the routing mechanisms. The distribution of false routing information allows the potential of unintended network routing loops, denial of service attacks, or other non functional routes. These attacks may hinder or prohibit the communication vital to fulfilling the mission of networked nodes. It is therefore critical for nodes to dynamically determine the validity of routing information prior to making routing decisions. With authentication and encryption mechanisms, secure routing protocols have been developed to ensure properties such as confidentiality and integrity.

These protocols require a centralized trusted third party, which is impractical for MANETs.

A. *Our proposed work has following key point to be solved-*

- Performance evaluation of the routing protocols
- (Table driven and dynamic) in sensor network with respect to energy consumed.
- Calculation of optimal route of each node during transmission and trust management based on behaviour of nodes using Routing table created during simulation.

B. *Proposed solution based on three parameters for best routing selection (less overhead of energy)*

- Minimum Delay of the path
- Maximum packet delivery ratio
- Max residual energy remain

Observing a node's behaviours is an effective mechanism to determine whether this node can be trusted. Meanwhile, we find that the conjunction of subjective passive acknowledgment and node's capability level on providing services can give an effective indication of a node's behaviours of cooperation

Step 1: Packet Forwarding Ratio (PFR)
Author divides into two categories-

- Data FR and
- Control FR

Step 2: Route Trust (RT)

Control Overhead (CO) by each node (additional metrics) checked by using the step1. Otherwise the nodes are considered as malicious and it is removed from the network. If the nodes satisfy the conditions in step 1, these nodes are undergo the rating process and added to the source list. These newly added nodes are considered for the next data transfer.

IV. SIMULATION AND EVALUATION

We have used NS3 (Network Simulator 3) for simulation. NS is a c++ script interpreter that has a simulation event scheduler and network component object libraries, and network setup module libraries. The simulated results show the malicious node identification in the network. In this the simulated model designed as such the source node receives the signal it performs the process and identifies the trusted and malicious nodes and routing is done that is the data packet

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

is transferred. And the performance metrics are analyzed by using graph. In this the simulated graph results are analyzed. The existing system, ASER [20], is compared with our proposed work. The main factors include energy consumption, memory overhead and packet delivery ratio.

A. *Energy Consumption:* Energy consumption is the usage of battery source. Energy overhead of monitoring involves−
   (i) the energy spent by the CPU for running algorithm
   (ii) the energy spent in sending/receiving packets related to monitoring such as

Neighbour discovery and malicious node detection announcements. The power is used to transmit and receive the packets. It is an flooding based technique, it does not retransmit any packets. It is done on the basis of on demand which improves the energy efficiency. This all reduces the energy consumption. FIG1 represents the energy consumption with respect to time. When compared to ASERT [20], the malicious node is found by using two phases. In our work it is done by using single phase MAC model.

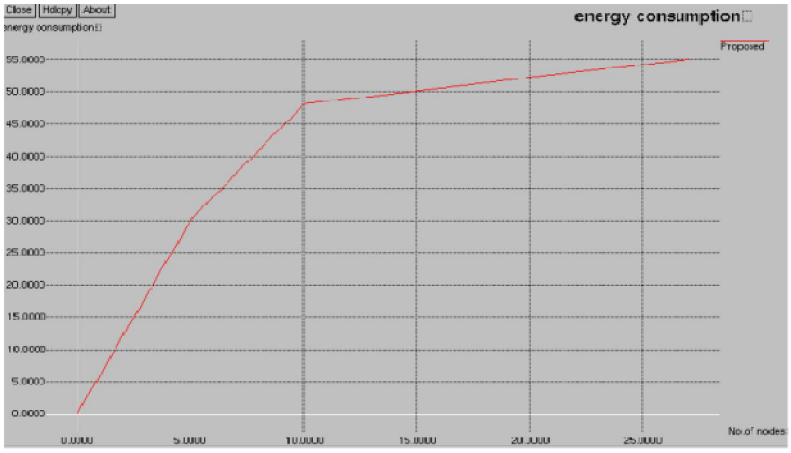

Figure 1: Energy Consumption

B. *Memory Overhead:* Memory overhead is the amount of memory it requires to store the values that is need for the process of finding malicious node. ASERT[20] it needs more memory space to store each nodes parameters. In our work the source node only has the list of trusted node. It establishes the routes when the node wants to transmit it. FIG2 deals with the memory overhead of our work with time.

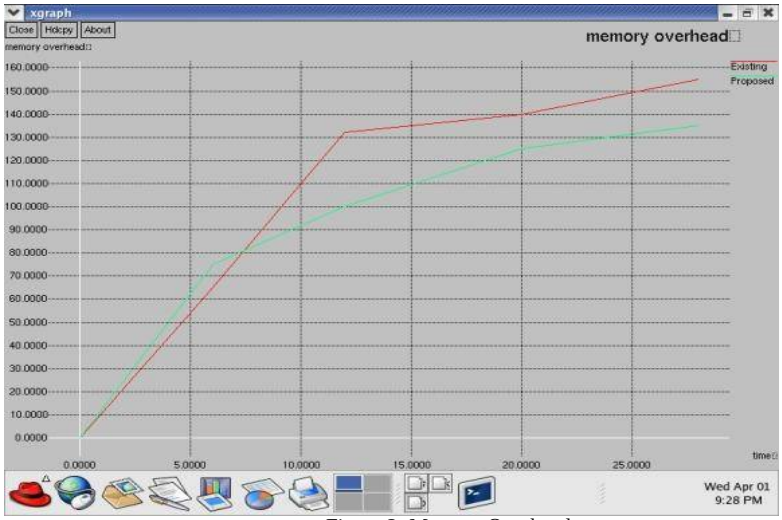

Figure 2: Memory Overhead

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

C. *Packet Delivery Ratio (PDR)*: PDR is defined as the number of data packets transmitted to the data packet received at the destination. The malicious nodes are identified accurately, the possibility of packets drop is minimum. Thereby the PDR is increased in our work. FIG 3 represents the PDR of our work with respect to number of nodes.

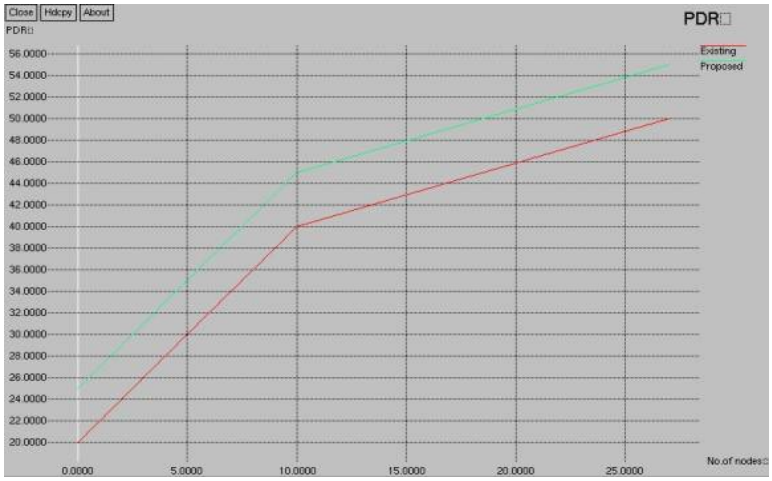

FIGURE 3: PACKET DELIVERY RATIO

V. CONCLUSION

In this paper we worked on Trust management is an important security service for WSNs, mainly because of their cooperative nature and their vulnerability to node compromise and misbehavior .The analysis of the characteristics and the security requirements of WSNs highlighted that the applicable trust management solutions should be light weight in terms of computational and communication requirements, yet power ful in terms of flexibility in managing trust between nodes of heterogeneous deployments. At the same time, the solutions should utilize the pre-deployment knowledge on the roles of the sensor node sand their trust associations..

REFERENCES

1. Pandey, A. and Tripathi, R. (2010). A Survey on Wireless Sensor Networks Security. International Journal of Computer Applications, 3(2),pp.43-49.
2. 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.
3. Latha, D, and Palanivel, K. 'Secure Routing Through Trusted Nodes In Wireless Sensor Networks – A Survey'. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 3.4 (2014): 8.
4. Kavitha, T., &Sridharan, D. (2010). Security vulnerabilities in wireless sensor networks: A survey. Journal of Information Assurance and Security, 5,
5. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1, 293–315Momani, M. and Challa, S. (2010). Survey of Trust Models in Different Network Domains. IJASUC, 1(3), pp.1-19.
6. 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.
7. 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
8. . 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.
9. 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).
10. Sheela, D., Nirmala S., Nath, S., & Mahadevan, G. (2011, July). A Recent technique to detect sink hole attacks in WSN. White paper, Anna University.
11. Marmol, F. G., & Perez, G. M. (2011). Providing trust in wireless sensor networks using a bio-inspired technique. Telecommunication System, 46,163–180.
12. Khalil, I., Bagchi, S., Rotaru, C. N., & Shroff, N. B. (2010). UNMASK: utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks. Ad Hoc Networks, 8(2), 148–164.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

13. Babu, S. S., Raha, A., &Naskar, M. K. (2011). A Direct trust dependent link state routing protocol using route trusts for WSNs (DTLSRP). Scientific Research, Wireless Sensor Network, 3,125–134.
14. Dhulipala, V., Karthik, N. and Chandrasekaran, R. (2012). A Novel Heuristic Approach Based Trust Worthy Architecture for Wireless Sensor Networks. Wireless PersCommun, 70(1), pp.189-205.
15. Yim, S. J., & Choi, Y. H. (2012). Neighbor-based malicious node detection in wireless sensor networks. Wireless Sensor Networks, 4, 219–225.
16. Gheorghe, L., Rughin, R. and tapus, N. (2012). Trust and Energy-aware Routing Protocol for Wireless Sensor Networks. In: The Eighth International Conference on Wireless and Mobile Communications. IARIA,.
17. Gheorghe, L., Rughiniş, R., Deaconescu, R. and Ţăpuş,N. (2010). Adaptive Trust Management Protocol Based on Fault Detection for Wireless Sensor Networks. In: The 2ndIntel. Conferences on Advanced Service Computing. IARIA.
18. Abduvaliev, Abror, Sungyoung Lee, and Young-Koo Lee. 'Simple Hash Based Message Authentication Scheme For Wireless Sensor Networks'. 5.
19. Devanagavi, Geetha D., N. Nalini, and Rajashekhar C. Biradar. 'Trusted Neighbors Based Secured Routing Scheme In Wireless Sensor Networks Using Agents'. Wireless PersCommun (2014): 1-28.

BIOGRAPHY

Pratishtha Gupta is a Research Scholar in the Computer Technology and Application, Gyan Ganga College of Technology. She received Bachelor of Engineering degree in 2012 from Guru Ghasidas Vishwavidyalaya A Central University, Bilaspur, C.G., India. Her research interests are Computer Networks (Wireless Sensor Networks).