International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Secure Routing in Wireless Sensor Networks through the Identified Trusted Node

D. Latha[1], K. Palanivel[2]

[1]Department of Computer Science, Pondicherry University, Puducherry-605014, India

[2]Computer Centre, Pondicherry University, Puducherry-605014, India

Abstract: ***Wireless Sensor Network (WSN) are the emerging and challenging technology with low processing and battery power. Security becomes a major issue in WSN; because of its wireless nature it is prone to various types of attacks and losing of data packet. Secure routing is important to avoid this type of issues. They are many techniques are available to provide secure routing to WSN. In the proposed work, our main aim is to find the trusted node and routing is done through the node to provide secure routing. The trusted node is identified by using MAC model and it is rated. And also giving the un trusted node a chance to relay prove its identity. It provides the security features with minimum overhead and energy efficiency.***

Keywords: Wireless Sensor Networks, Secure Routing, Secure Hash Algorithm

1. 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 un trusted 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, section 3 discuss the proposed method, section 4 deals with the Simulation and Analysis, section 5 comprises of conclusion.

2. 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 algorithm are not needed to find the shortest path, it is easily found, 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, 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.

3. Proposed System

The sensor node in the wireless sensor network wants to send data to the destination node (sink node). The routing has to be done in a secure way that the sensed data reach the sink without modification and also free from attack. So secure routing is done. It is done by finding the trusted node by our proposed work. The work consists of 4 steps, which are described below.

3.1 Step1: MAC model

In this the Secure Hash Algorithm is used [19]. We use SHA-1 hash function to compute message authentication code of a given message M. The pseudo code for SHA algorithm for MAC model is given in ALGORITHM1. Source node computes MAC (Message Authentication code) with the help of secret key over message M, and then sends it to neighbour node. The neighbour node computes MAC of received message using the secret key of source which is shared with sensor node by the source node. Then the MAC values are computed. If the computed MAC values are matched with the created MAC, it sends the ACK to the source node. If the ACK does not received by the node the node consider as the un trusted node, the nodes are kept in a separate list. The remaining un trusted nodes that are kept in the separate list they will undergo the separate process that is discussed later (step 4). The trusted nodes identified by this step undergo the next process as Rating.

Algorithm1 : SHA for MAC model

Start
Source: compute MAC $_K$ (M)= H_K(M)
Source: transmit M and MAC $_k$ (M)
Neighbour node : gets M and MAC $_k$ (M)
Neighbour nc 'e: compute MAC $_K$'(M)=H_K'(M)
Neighbour node : compare MAC $_K$' and MAC $_K$
If compare MAC $_K$' = MAC $_K$ then
Neighbour node : trusted

Else

Neighbour node : Un trusted

End if

End

3.2 Step2: Rating

The trusted nodes are rated on the basis of the amount of data transmission they accomplish and their friendship with other nodes in the network. The rating is done by the data rating and friend rating. Data rating based on the data packets transfer through the node. That is based on the packet size. Data rating portrays its capacity to transfer the data packets. Friend rating is done through the account of friendship of a node with other nodes in the network. If a node wants to calculate its rating, its behaviour with the neighbour node is noted and it is rated. Now every node has the Data rating and friend based rating. Net rating is calculated from that. This rating helps to identify how good the trusted node. Now the trusted node along with its rated value is available. The list is shared with source sensor node and to its destination (sink node).

3.3 Step3: Routing

The source has the list of trusted node. if the source node receives the signal it starts to route the data packets through the nodes which are identified and rated by the above steps. Now the routing is done through the trusted node that makes the routing more secure. Therefore we avoid the attacks and information loss. The trusted node list are shared to the destination so that it assures the information is from the trusted node and also the sensed data is from the node with the high rating is considered as accurate sensed data.

3.4 Step4: Cross Check

The un trusted node which are in the separate list are identified by MAC model are not completely removed from the entire network and it is given a chance to check whether it is really malicious or not. In step1 if the MAC matches it sends the ACK back to the source within the specified period. But there is possibility that the MAC matches, and the ACK does not receive the source node within the time or it may lost because of its wireless nature. This condition may lead to trusted node is identified as malicious node. Therefore, the cross check is needed. This process is separate. Consider the Node N1, N 2, N 3 which are identified as an un trusted node by MAC model. In this N1 sends packet and forwards it to N2, and N2 forwards it to N3, once N3 received the packet it send back the ACK to N1. If the node receives ACK, then the nodes are again 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.

4. Simulation and Evaluation

We have used NS2 (Network Simulator 2) for simulation. NS is an Object-oriented Tcl(Otcl) script interpreter that has a simulation event scheduler and network component object libraries, and network set_up module libraries. The simulated results show the malicious node identification in the nertwork. 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 is transferred. And the performance metrics are analysed by using graph. In this the simulated graph results are analysed. The existing system, ASER[20], is compared with our proposed work. The main factors include energy consumption, memory overhead and packet delivery ratio.

4.1 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 neighbor 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.

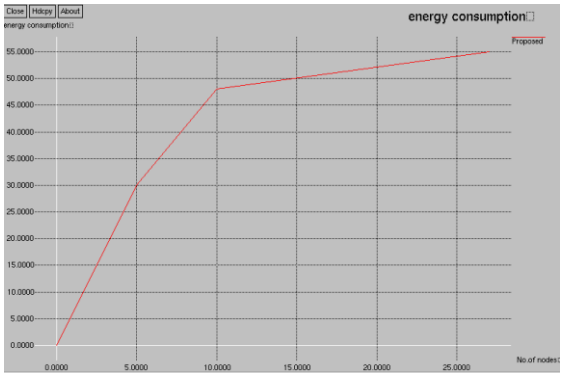

Figure 1: Energy Consumption

4.2 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.

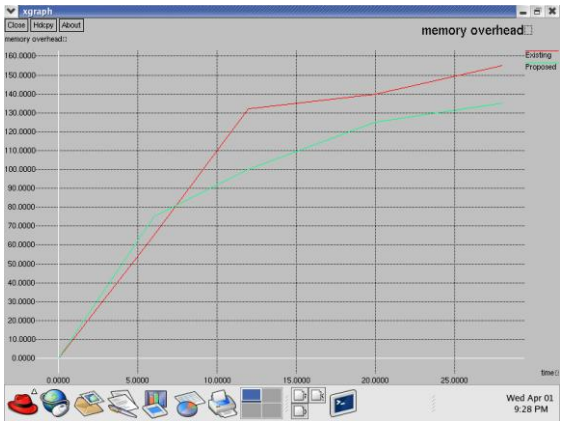

Figure 2: Memory Overhead

4.3 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.

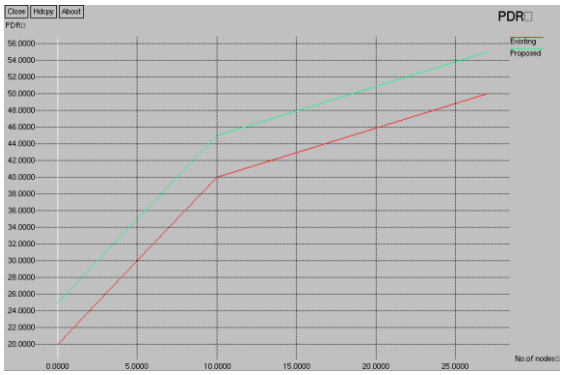

Figure 3: Packet Delivery Ratio

4.4 Delay

The delay of a network specifies how long it takes for the data to travel across the network from source node to destination. The time required to compute the MAC model, finding the malicious nodes also determines the delay of the network. In our work the malicious nodes are identified effectively, so that the data packets travel through the trusted node minimize the delay in network. FIG 4 depicts the delay with respect to our work.

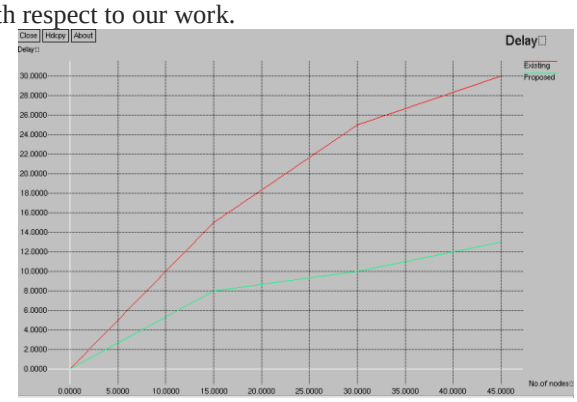

Figure 4: Delay

4.5 Security Analysis

The security features include confidentiality, integrity authentication. We achieve this features and free from network attacks by routing through identified trusted nodes. In our work, we use SHA-1 Algorithm. In this the Hash values are unique and it is difficult to determine the MAC values. Un authorized person should not compute the MAC without knowing the shared key. Thereby computing the MAC, the nodes behaviour is determined, this ensures the node trustworthy nature.

5. Conclusion

WSN are deployed in hostile environment and because of its wireless nature it is subjected to various kinds of attacks, information loss and modification. It is important in WSN the sensed data packets should reach the destination within the particular time and also the data packets should not undergo any modification. Secure routing is the way to avoid this kind of problems. In WSN secure routing is done to route the data packets securely without modification. Therefore trusted nodes are identified and routing is done through it.

In our work, The trusted nodes are identified by the MAC model and it is rated. MAC model effectively identifies the un trusted node by using SHA algorithm. The data packets are routed through the trusted node. Trusted node gives security features such as confidentiality, integrity and authentication because it is identified by MAC model. The nodes are rated which is based on data transfer and friendship with other nodes, this provides complete information of the node. And also the un trusted nodes are given a chance to prove it is really malicious or not. The trusted nodes are identified effectively. The nodes are free from attacks.

Therefore the data packets reach the destination without loss and modification because it routes through the trusted node. Thus makes the routing secure. The security goals are achieved with less memory overhead, energy consumption and improve the Packet delivery ratio.

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, 31–44.

[5] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks*, *1*, 293–315.
[6] Momani, M. and Challa, S. (2010). Survey of Trust Models in Different Network Domains. IJASUC, 1(3), pp.1-19.
[7] 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.
[8] 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.
[9] 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.
[10] 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).
[11] Sheela, D., Nirmala S., Nath, S., & Mahadevan, G. (2011, July). A Recent technique to detect sink hole attacks in WSN. White paper, Anna University.
[12] Marmol, F. G., & Perez, G. M. (2011). Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommunication System*, *46*, 163–180.
[13] 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.
[14] 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.
[15] Dhulipala, V., Karthik, N. and Chandrasekaran, R. (2012). A Novel Heuristic Approach Based Trust Worthy Architecture for Wireless Sensor Networks. Wireless Pers Commun, 70(1), pp.189-205.
[16] Yim, S. J., & Choi, Y. H. (2012). Neighbor-based malicious node detection in wireless sensor networks. Wireless Sensor Networks, 4, 219–225.
[17] 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,.
[18] Gheorghe, L., Rughiniş, R., Deaconescu, R. and Ţăpuş, N. (2010). Adaptive Trust Management Protocol Based on Fault Detection for Wireless Sensor Networks. In: The 2nd Intel. Conferences on Advanced Service Computing. IARIA.
[19] Abduvaliev, Abror, Sungyoung Lee, and Young-Koo Lee. 'Simple Hash Based Message Authentication Scheme For Wireless Sensor Networks'. 5.
[20] Devanagavi, Geetha D., N. Nalini, and Rajashekhar C. Biradar. 'Trusted Neighbors Based Secured Routing Scheme In Wireless Sensor Networks Using Agents'. Wireless Pers Commun (2014): 1-28.