Secure Routing based on Trust Sensing for Wireless Sensor Network

G. Praveen Babu[1], A. Sushmitha[2]

[1]Associate Professor of Computer Science & Engineering

[2]M.Tech Student of Computer Networks & Information Security

[1]School of Information Technology, JNTUH, Hyderabad, India
[1]pravbob@jntuh.ac.in, [2]94sushmitha94@gmail.com

Abstract

A secure routing based on trust sensing is proposed in this paper in view of the severe attacks caused because of the limited resources and poor deployment of Wireless Sensor Networks (WSN) environment on data transmission. A secure routing with lightweight features and the ability to prevent many of the common attacks concurrently can further be enhanced by considering the Quality of Service (QoS) metrics and the Trust value into account. Analytic hierarchy process is used to analyze and build trust calculation model based on direct trust, indirect trust. Performance analysis and simulation results show that SRTS can improve the security and efficiency of WSN.

This paper analyzes the behavior of sensor nodes, including the movement and energy consumption of sensor nodes. The trust value of sensor node is calculated using these characters, and then the trust value of route is calculated and the trust calculation model of network is established to get the optimal route between the source node and the destination node. The QoS metrics and trust value are considered together as the routing metrics to present an enhanced routing algorithm.

Secure routing based on trust sensing with intrusion detection mechanism designing and working process is described. The proposed routing algorithm is applied to the secure routing to obtain the effective and reliable transmission of data.

Keywords: Wireless Sensor Network, Trust Value & optimal route.

1. Introduction

Wireless Sensor Network (WSN) is collection of nodes where each node has its own sensor, Transmitter, receiver and processor. The WSN deploys a large number of low-cost sensor devices distributed over an area of interest. Being of low cost such sensors are deployed densely throughout the area to monitor specific event. 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.

WSN provides a bridge between physical and virtual worlds. Sensor have limited sensing region, processing power and energy. Nodes of the sensor network comprises of four subsystems: sensor subsystem for sensing the environment, the processing subsystem for accomplish the computations on the sensed data, and the communication subsystem is perform the message exchange with neighboring 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 energy waste are ideal listening, control overhead, collision and overhearing in medium access unlike MAC protocols, WSN schemes must support sleep modes to maximize energy efficiency during radio inactivity. 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.

The network attacks can be divided into routing protocol attacks and trust model attacks according to different attack targets. The routing protocol attacks are more severe in WSN as it is a Multi-hop relay routing, than in the general wireless communication network. Generally, routing protocol attacks can be classified into soft attacks and hard attacks according to the behavior of attackers.

Soft attacks mean that malicious or selfish nodes steal or destroy the relay data by pretending fictitious route, examples are: black hole attack provides false available channel information in the routing request, gray hole attack drops some data packets deliberately, sinkhole attack fabricates native resources, wormhole attack constructs false links by conspiracy, sniffing attack eavesdrops routing information by analyzing network traffic, as well as sybil attack that forges multi-identity.

Hard attacks mean that malicious nodes damage the information transmission by destroying the existing transmission resources, such as: DoS attack that exhausts the resources by introducing heavy traffic than the maximum processing limit of attacked objects, tampering attack that tampers routing data and replay attack that involves passive imprisonment of the data and its succeeding retransmission occupies bandwidth maliciously.

Advantages of secure routing based on trust sensing (SRTS):

1. The proposed routing algorithm is applied to the secure routing mechanism to achieve the efficient and reliable transmission of data.
2. At the same time, the maintenance process of SRTS is also presented to further ensure the security of data transmission.
3. SRTS not only improves the security of information for multi-hop communication network, but also reduces the routing overhead in WSN effectively.
4. Low computational cost.
5. Improves the average packet delivery rate.
6. Handles gray hole and bad mouthing attacks.

2. Related Work

WSN with the characteristic of low cost, rapid deployment and self-organization plays a vital role in facilitating the services of smart city. The ubiquitous sensor nodes can both collect the physical information of urban environment and control the public and private facilities in the context of smart urban environment. However, the multi-hop routing is vulnerable to various types of attacks due to the open, distributed and dynamic characteristic of WSN, which has a serious impact on data and information security. At present, the existing secure routing algorithms are usually directed against specific

malicious or selfish behavior attacks, since they mainly rely on encryption algorithms and authentication mechanisms, which are not suitable for the multi-hop distributed and energy-constrained WSN.

To reduce the likelihood of compromised or malicious nodes being selected (or elected) as cluster heads [3], the self-election is allowed for the first sets of cluster-heads. When the clusters are established the cluster head schedules the transmission of each member in a TDM manner and inform all the members. When current cluster head's work for a predetermined amount of time, the battery power level falls below a predetermined threshold or, it broadcasts (within the cluster) a new election message. Then new cluster head elected by all the nodes by using secret ballot.

A detection route refers to a route without data packets whose goal is to convince the adversary to launch an attack so the system can identify the attack behavior and then mark the black hole location [4]. Thus, the system can increment the trust of nodes in successful routing and decrement the trust of suspicious nodes. Through the nodal trust can be quickly obtained by active detection routing, and the data route can effectively guide in choosing nodes with high trust to bypass black holes.

To prevent attack, trust values of nodes is considered before making decisions on data forwarding. When any node is compromised that node can't have higher trust value and thus it can't participate in communication [6]. The trust manager computes trust level of each neighbor based on various events such as trust level of each neighbor, broadcast nature of base station and discovery of network loops. Trust manager gives complete security to the communications in WSN. This is possible as the trust manager can determine the trust level of nodes and make appropriate routing decisions. Adversaries can't reach base station as they do not have trust.

3. Proposed Work

This paper analyzes the behavior of sensor nodes, including the movement and energy consumption of sensor nodes. The trust value of sensor node is evaluated according to these characters, and then the trust value of route is calculated and the trust calculation model of network is established to get the optimal route from the source node to the destination node. At the same time, the trust value and QoS metrics are combined as the routing metrics to present an optimized routing algorithm.

3.1. System Model

The watchdog is used to detect the behaviors of malicious nodes in the network. The absorbed behaviors are considered for the calculation of mutual trust among sensor nodes and used as the basis of trust calculation; td(x, y) denotes the trust value y for x.

3.2. Establishment of Trust Model

To analyze and establish trust calculation model, Analytic Hierarchy Process (AHP) is adopted. The trust model between two nodes (including direct trust value, indirect trust value and incentive factor) is taken to construct the trust calculation model of the whole multi-hop route to judge the secure route of data transmission.

- Direct Trust Calculation of Nodes: The behaviour of sensor nodes can be monitored by neighbour nodes in WSN. Since sensor nodes are highly constrained in

computing power, memory, energy, and bandwidth, it is not enough to judge the behaviour of nodes only by monitoring the trust value of nodes; therefore, this study will combine behaviour with energy to evaluate the trust value of nodes comprehensively.

- Indirect Trust Calculation of Nodes: The trust relationship implemented by other neighbours in the target node's connected domain. Similar to the direct trust construction model, the indirect trust value is combination of the indirect behaviour trust value and the indirect energy trust value.

  Since energy is an objective parameter, the indirect energy trust value is the same as the direct energy trust value. Only the indirect behaviour trust value of node is considered here. If the direct connected domain of target node y in the network is Cy, itd(x, y) [1] represents the indirect trust value calculated by node x according to the information provided by all the nodes in Cy.

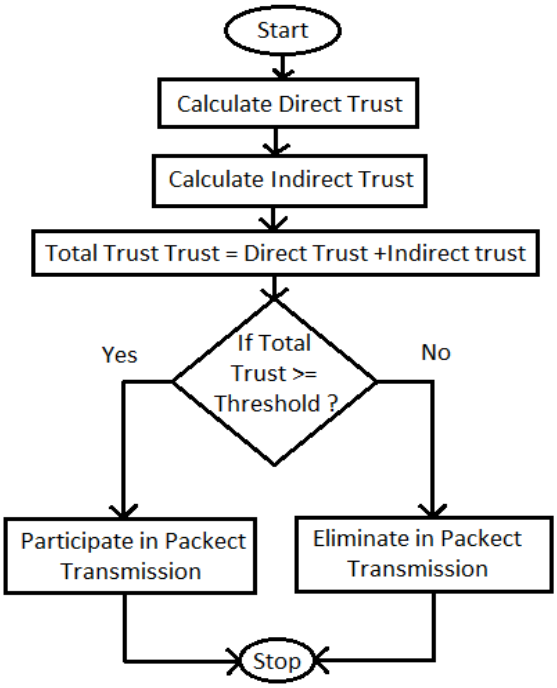

Figure 1. Trust calculation process

This model is established to punish the malicious nodes while encouraging the nodes to cooperate. If the node does not participate in network cooperation, then the trust value of node will be reduced. The node is considered as a malicious node or a failure node and will be removed out of the network when its trust value is below a certain level. If the node already has higher trust value, the node is still highly involved in the cooperation in the networks, and then the network will consider the node as a malicious node and remove it out of WSN directly.

3.3. Route Trust Computation

When the nodes in the network complete the route discovery process according to the adopted routing protocol, it will not directly determine the route and enter the information transmission phase, but calculate the trust value of route firstly. In general, the design of trust calculation for route must meet the rules below.

1. Credible message cannot be increased through dissemination;
2. The destination node is identified as credible node, and its initial trust value will be set as 1.

3.4. Routing Selection

Optimal credible route set obtained based on other QoS metric priority and continue to traverse the route selection process according to the trust and energy levels of the nodes, until the optimal route satisfying both the trust value and QoS metrics is obtained.

4. The Scheme of SRTS

The Secure Routing based on Trust Sensing (SRTS) handle common network attacks. An optimized routing is proposed by considering the trust value and other QoS parameters.

4.1. Initialization of Network

The node with higher initial trust value is chosen as the cluster head. The higher the node's trust value is, the higher its energy is, and the longer the node lifetime is, which is more favorable for the stability of cluster structure.

In this phase, the nodes are non-clustered, and each node has a random initial trust value. Each node will monitor the behaviors of neighbor nodes and exchanges their initial trust value with each other to select the new cluster head according to the cluster head selection mechanism.

4.2. Construction of Route

The initialization of network is finished after determining the cluster head according to trust values, then the transmission link need to be constructed. The SRTS will only select the suggestions provided by neighbor nodes of the evaluated node, which control the recommended range and reduce the communication overhead in the process of information transmission. In addition, the combination of direct trust and indirect trust can effectively detect the nodes which give up relay forwarding to save energy, so as to expel selfish nodes or attack nodes from the credible route quickly.

Source node n0 transmits the trust request packet TRP to its neighbors (eg, node n2) when it is ready to transmit message to Sink node n11. The trust request packet is expressed as TRP= ⟨sid, rid, td(r)th, ts, sn, hc⟩, where 'sid' and 'rid' represent the identity of assessing node(sending node) and assessed node(receiving node), respectively. 'td(r)th' denotes the threshold of route trust. 'ts' denotes timestamp and 'sn' denotes the serial number of trust request packets. 'hc' represents the hop counter of TRP, hl is positive integer and decreases with the increasing of the number of forwarding. 'hc' should not be set too large in order to reduce the flooding overhead caused by the trust transmission.

Source node n0 is identified by 'sid' and neighbor node n2 which receives the TRP is identified by 'rid'. Upon receiving the TRP, node n2 need to check the freshness of the packet, and the request will be discarded if it is duplicate one, otherwise, the request will be forwarded to all the neighboring nodes of n2.

On receiving the trust request packet, the neighboring nodes (n1, n3) of node n2 will send the trust reply to node n0 in the reverse route. The neighbors will response to the

request only if they receive the fresh request which is not the repeated one and its hop count 'hc' is not decremented to zero.

After receiving the replies provided by the neighboring nodes of node n2, node n0 will combined direct trust, indirect trust and evaluate the trust status of node n2.

Based on this evaluation, node n0 decide whether n2 can be a relay node according to the constraint condition of trust. Node n0 can obtain a credible forwarding set (n2, n3) and according to the constructed trust calculation model, send routing requests to the node.

The above steps are repeated to find the credible nodes in the optimal route from the source node to destination node. The intermediate nodes receive the trust requests and send back the replies to obtain the optimal route.

Once the optimal route is constructed according to the routing algorithm, the sink node will reply to source node through the intermediate credible nodes in reverse route.

The source node will send the packets to destination through the optimal route constructed with the intermediate credible nodes.

4.3. Maintenance of Route

Route maintenance is used to handle the credible route repair caused by node movement or failure in WSN and the credible route update when new nodes are joined.

5. Simulation Results and Performance Evaluation

NS2 simulator is used in the project to analysis the node performance. 50 nodes are distributed in the area of 150m × 150m and every tabularized below in table. Node observes the behaviors of its neighboring nodes to calculate their trust value. The simulation parameters are

Table 1. Experiment Parameters

Parameters	Values
Simulator	NS2
Simulation Time	20ms
Number of nodes	50
Routing Protocol	DSR
Initial Energy	200J
Transmission Power	1.0J
Receiving Power	0.5J
Simulation Area	1000×1000
Channel	Wireless
Radio Model	Two Ray Ground Model
Antenna Type	Omni Antenna

5.1. Packet Drop

Packets of data travelling across a network fail to reach their destination. Packet loss is either caused by errors in data transmission, typically across wireless networks, network congestion or by a packet drop attacks. Packet drop is measured as a percentage of packets drop with respect to packets sent.

The packet arrives for sustain period in a specific path or link at a rate greater than it is possible to send through, then packets will be dropped. To avoid this Scenario SRTS will consider the energy levels of the nodes in the routing path, to balance the distribution of load in the network. The clustering is also one of the efficient techniques adopted by SRTS to distribute the load evenly on node of the WSN.

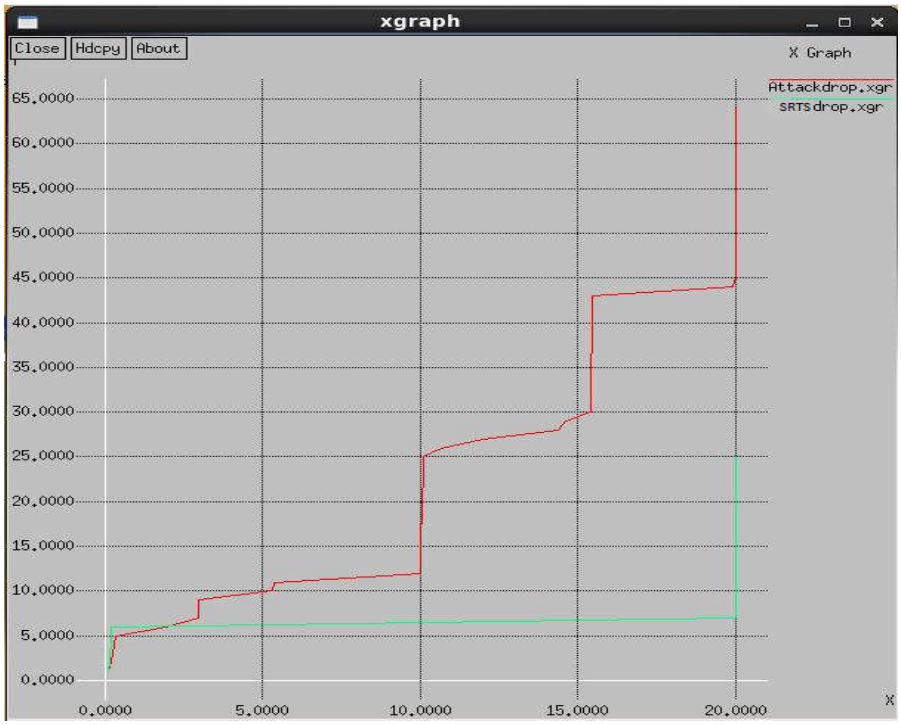

Figure 2. The impact of packet drops

The figure 2 shows the packet drops comparison between gray hole attack scenario and with proposed Secure routing based on trust sensing scheme.

5.2. Packet Delivery Ratio (PDR)

The effectiveness of data delivery is indicated by the PDR and is affected by errors in communication, buffer overflow, or failure of nodes. If number of packets is P which is needed to reach the sink node and number of packets p which have successfully reached sink. Then successful packet delivery ratio is as follows, R = p/P, The goal is maximize the ratio i.e., max(R) = p/P. Achieving a reasonably good delivery performance using WSN, an energy-constrained environments is difficult.

Figure 3. The impact of packet delivery ratio

The figure 3 shows the packet delivery ratio comparison between the gray hole attack scenario and the proposed Secure routing based on trust sensing scheme and it is found that the red graph on x-axis represent the PDR in existing network which is decreasing with time and green graph represent the PDR in SRTS is maintained almost stable throughout the simulation.

5.3. Network Performance Analysis

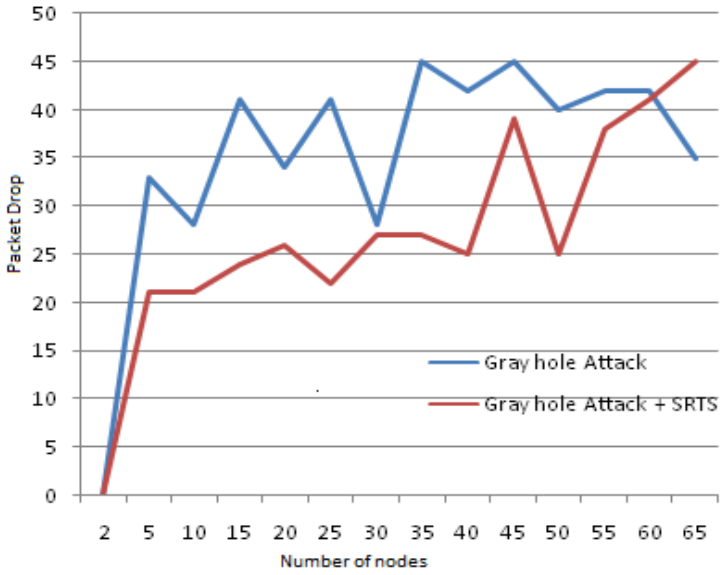

Figure 4. Packet drops in gray hole and SRTS

The figure 4 shows the packet drops comparison between gray hole attack scenario and with proposed Secure routing based on trust sensing scheme with varying number of nodes participating in the network. This analysis is to know the maximum number of node that can participate actively in the packet transmission without degrading the SRTS performance. The maximum allowable number of node in SRTS is 60, beyond this count the performance changes.

6. Conclusion & Future Scope

WSN is a very important part of modern communication systems. Trust sensing routing protocol for WSN is an effective way to improve security. Therefore, the study of trust sensing routing protocol is extremely vital. This paper presents a trust sensing based mostly secure routing mechanism to handle common network attacks. An optimized route is constructed by considering the trust value and QoS parameters. The simulation results presented in the paper depicts the trust sensing based secure routing mechanism certainly reduces routing delays and further enhances the data reliability. The network performance can be further analyzed by considering the varying number of attacking nodes and corresponding packet drops in the network. In future this work can be extended by usage of better intrusion detection system designed especially for WSN which may lead to better research results.

References

[1] N. Marlon, C. Jose, A. B. Campelo, O. Rafael, V. C. Juan, and J. S. Juan, ”Active low intrusion hybrid monitor for wireless sensor networks,” Sensors, vol. 15, no. 3, pp. 23927-23952, 2015.

[2] G. Uttam G, and D. Raja, ”SDRP: secure and dynamic routing protocol for mobile ad-hoc networks,” IET Networks, vol. 3, no. 2, pp. 235-243, 2014.

[3] X. Du, and H. Chen, ”Security in Wireless Sensor Networks,” IEEE Wireless Communications, vol. 15, no. 4, pp. 60-66, 2008.

[4] Y. X. Liu, M. X. Dong, O. Kaoru, and A. F. Liu, ”ActiveTrust: Secure and trustable routing in wireless sensor networks,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 2, pp. 2013-2027, 2016.

[5] J. P. Yao, S. L. Feng, X. Y. Zhou and Y. Liu, ”Secure routing in multihop wireless ad-Hoc networks with decode-and-forward relaying,” IEEE Transactions on Communications, vol. 64, no. 13, pp. 753-764, 2016.

[6] Dhanunjayudu.K, and Mahesh.B, ”Trust-Based Secure And Energy Efficient Routing Framework For WSNS, ” International Journal of Computer Trends and Technology- volume 5 number 1 – Nov 2013

[7] Marc Greis' Tutorial for the UCB/LBNL/VINT Network Simulator “ns” http://www.isi.edu/nsnam/ns/tutorial/index.html

[8] M. E. Mahmoud, and X. Shen, ”Trust-based and energy-aware incentive routing protocol for multi-hop wireless networks,” In Proceedings of the IEEE International Conference on Communications (ICC ’11), Budapest, Hungary, Jun. 2008, pp. 88-91.

[9] K. B. Sourav, and M. K. Pabitra, ”SIR: a secure and intelligent routing protocol for vehicular ad hoc network,” IET Networks, vol. 4, no. 6, pp. 185-194, 2015.