A Trust Based Sensor Protocol for Information Dissemination in a Point to Point Media

Nimmy George
M.Tech Student, Dept of CSE
Viswajyothi College of Engineering and Technology, Muvattupuzha, Kerala
nimmy4ever@gmail.com

Abstract

Securing the information dissemination is an important issue in wireless sensor network. Previously, there is no available work on the integrated design of trust model and SPIN-PP protocol (sensor Protocols for Information via Negotiation) for information dissemination in wireless sensor networks. In this paper, to improve the quality of this a trust based sensor protocol for information dissemination in a point to point media is proposed. Here, first find out trust values of all the nodes by the trust model. In the existing trust models each node's trust table contains trust value of all its neighbors. But in this proposed solution each node's trust table contain only its own value. So there is no need for broadcasting the trust values of all the nodes. This will reduce the transmission overhead over the network. Then SPIN-PP is used for information dissemination over the network. Here the information can be send to the nodes with trust value higher than or equal to the threshold.

Key Words: *Wireless Sensor Network,SPIN-PPTrust model, information dissemination*

1. INTRODUCTION

Wireless sensor network consist of spatially distributed autonomous sensors to monitor physical or environmental conditions such as temperature, sound, motion, vibration and pressure. Security has an important role in the routing procedure. The WSNs are characterized by limited energy, bandwidth, and memory capacity. This will impose strict limitations in the implementations of security mechanism. The security requirements [1] are user authentication, confidentiality, node verification, integrity. Unfortunately security solutions for other networks are not applicable to WSNs. So, to defend against attacks new security solutions are needed.

Wireless sensor networks improve sensing accuracy by providing distributed processing of vast quantities of sensing information. Each sensor node operates autonomously with no central point of control in the network, and each node bases its decisions on its mission, the information it currently has, and its knowledge of its computing, communication and energy resources. Compared to today's isolated sensors, tomorrow's networked sensors have the potential to perform with

more accuracy, robustness and sophistication. Several obstacles need to be overcome before this vision can become a reality. These obstacles arise from the limited energy, computational power, and communication resources available to the sensors in the network.

• Energy-Because wireless sensors have a limited supply of energy, energy-conserving communication protocols and computation is essential.
• Computation- Sensors have limited computing power and
therefore may not be able to run sophisticated network protocols.
• Communication- The bandwidth of the wireless links connecting sensor nodes is often limited, on the order of a few hundred Kbps, further constraining inter-sensor communication.

A wide variety of security attacks such as black-hole and grey-hole attacks address the information dissemination. In the black hole and grey-hole attacks the selfish nodes are refused to forward all or part of the traffic received from its neighbors. These kinds of attacks can be avoided by using the proposed solution.

In the trust model each node establishes trust relationship with each other and base their routing decisions not only on pure or geographical information but also on their expectation that their neighbors will sincerely cooperate. Trust is the confidence of a node hi that a node hj will perform as is expected. The method for obtaining trust information defining each node's trustworthiness are termed as trust models .The concept is to create on each sensor a trust repository table which will maintain and handle the information. Trust values are computed between 0 and 1. All these schemes are aim to improve the security and thus to increase the throughput.

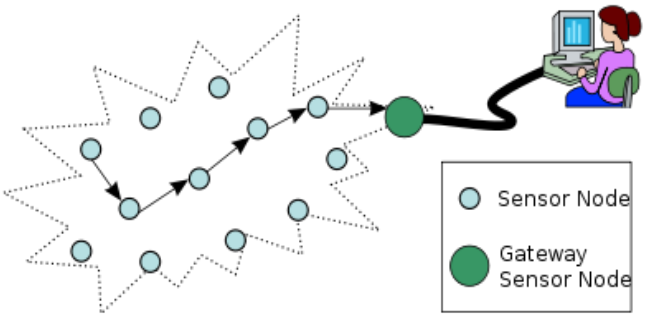


Figure 1.Wireless Sensor Network

SPIN is used to disseminate information among sensors in an energy-constrained wireless sensor network. Nodes running a SPIN communication protocol name their data using high-level data descriptors, called meta-data. They use meta-data negotiations to eliminate the transmission of redundant data throughout the network. In addition, SPIN nodes can base their communication decisions both upon application-specific knowledge of the data and upon knowledge of the resources that are available to them. This allows the sensors to efficiently distribute data given a limited energy supply. There are mainly four specific SPIN protocols .The SPIN-PP and SPIN-EC are optimized for a point-to-point network, and SPIN-BC and SPIN-RL, which are optimized for a broadcast network. SPIN-PP is mainly used for to overcome the problems such as implosion, overlap and resource blindness.

• Implosion - In classic flooding, a node always sends data

to its neighbors, regardless of whether or not the neighbor has already received the data from another source. This leads to the implosion problem. For example, node A starts out by flooding data to its two neighbors, B and C. These nodes store the data from A and send a copy of it on to their neighbor D. The protocol, thus, wastes resources by sending two copies of the data to D. It is easy to see that implosion is linear in the degree of any node.

•Overlap- Sensor nodes often cover overlapping geographic areas, and nodes often gather overlapping pieces of sensor data. Overlap is a harder problem to solve than the implosion problem – implosion is a function only of network topology, whereas overlap is a function of both topology and the mapping of observed data to sensor nodes.

• Resource blindness - In classic flooding, nodes do not modify their activities based on the amount of energy available to them at a given time. A network of embedded sensors can be "resource-aware" and adapt its communication and computation to the state of its energy resources.

In the proposed design, first find out the trust values of all nodes in the transmission range. Then SPIN-PP protocol is used for information dissemination on these nodes. This will reduce chance of sending data to the attacker nodes in the network.

The rest of the paper is organized as follows. In section 2, perform a study on the previous work. Section 3 specifies the proposed solution. Then paper is concluded in the next section.

II. PREVIOUS WORKS

There are many trust based models [2] [3] [4] [5] [6] are used for finding out the attacker nodes. In Some previous approaches the trust establishment is realized in a centralized manner. All these methods are used different parameters as metrics for calculating the trust value. There is no available work on trust based sensor protocols for information dissemination. In the existing trust models the trust values of all the nodes are broadcasted over the network. This will increase the transmission overhead and delay of this model. So the trust model used in the proposed solution, each node calculates its trust value and stored in its own table.

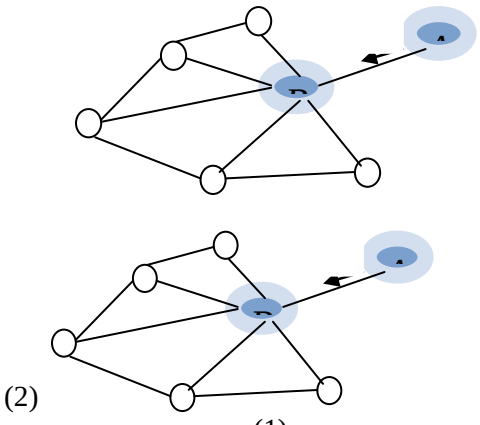
The existing approach [8] used in the proposed integrated design; the trust model is a fully distributed scheme. This trust model is suitable for the ad-hoc and wireless sensor networks. The concept is to create on each sensor a trust table which will maintain and handle trust and reputation information about each neighboring node. In the trust table values regarding a number of events are stored. Here the aspects to monitor are packet forwarding, network layer ACK, confidentiality, integrity, authentication, remaining energy. Then based on these values, an overall cost function is calculated and then store the value in its trust table.

The SPIN-PP [7] is used for information dissemination in wireless sensor networks. SPIN-PP, is optimized for a networks, using point-to-point transmission media, where it is possible for nodes *A* and *B* to communicate exclusively with each other without

interfering with other nodes. SPIN nodes use three types of messages for communication.

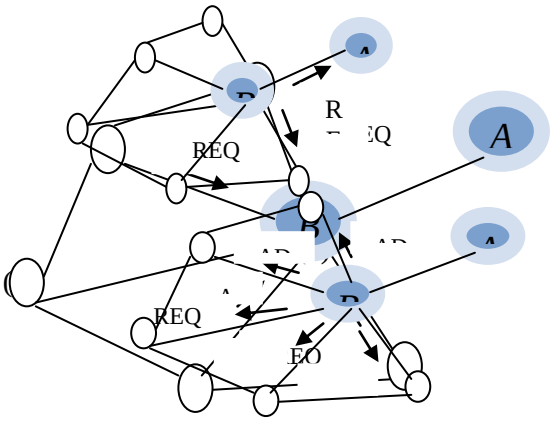
• ADV – new data advertisement. When a SPIN node has data to share, it can advertise this fact by transmitting an ADV message containing meta-data.
• REQ – request for data. A SPIN node sends an REQ message when it wishes to receive some actual data.
• DATA – data message. DATA messages contain actual sensor data with a meta-data header.

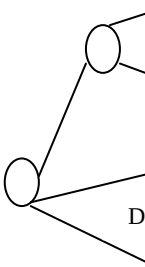
The SPIN-PP protocol works in three stages (ADV–REQ–DATA), with each stage corresponding to one of the messages described above. The protocol starts when a node advertises new data that it is willing to disseminate. It does this by sending an ADV message to its neighbors, naming the new data (ADV stage). Upon receiving an ADV, the neighboring node checks to see whether it has already received or requested the advertised data. If not, it responds by sending an REQ message for the missing data back to the sender (REQ stage). The protocol completes when the initiator of the protocol responds to the REQ with a DATA message, containing the missing data (DATA stage). Figure 2 shows an example of the protocol. Upon receiving an ADV packet from node A, node B checks to see whether it possesses all of the advertised data (1). If not, node B sends an REQ message back to A, listing all of the data that it would like to acquire (2). When node A receives the REQ packet, it retrieves the requested data and sends it back to node B as a DATA message (3). Node B, in turn, sends ADV messages advertising the new data it received from node A to all of its neighbors (4). It does not send an advertisement back to node A, because it knows that node A already has the data. These nodes then send advertisements of the new data to all of their neighbors, and the protocol continues.



(2)

(1)





(5)

Figure 2. The SPIN-PP protocol. Node A starts by advertising its data to node B (1). Node B responds by sending a request to node A (2). After receiving the requested data (3), There are several important things to note about this example. First, if node B had its own data, it could aggregate this with the data of node A and send advertisements of the aggregated data to all of its neighbors (4). Second, nodes are not required to respond to every message in the protocol. In this example, one neighbor does not send an REQ packet back to node B (5). This would occur if that node already possessed the data being advertised.

The main disadvantage of the trust model is that there is no specific protocol for routing procedure. And in the case of SPIN-PP, during the information dissemination some nodes in the routing path will slow down or refused to forward the information. If we are sending information to those nodes that nodes will refused to forward the information. To find out such nodes trust based SPIN-PP is used. This will provide more security. Previously, there is no available work on the integrated design of trust model and SPIN-PP protocol. So, this will avoid the attacker nodes from the information dissemination procedure.

III.TRUST BASED SENSOR PROTOCOL FOR INFORMATION DISSEMINATION IN A POINT TO POINT MEDIA

It is the improved integrated design of trust model and SPIN-PP. The trust model is used to find out the trust value of all nodes in the

(6)

node B then sends out advertisements to its neighbors (4), who in turn send requests back to B (5), node B send its data to the nodes which does not hold the advertised data (6).

routing path. The SPIN-PP is used as the sensor protocol for information dissemination through the nodes.

The trust value of each node is calculated by the trust model. The main idea is to create on each sensor a trust repository which contains only the information about its own trust value. Broadcasting of the trust value is avoided here to reduce the delay. In this, each node calculates its own trust value. A threshold is set for the trust value. The nodes with trust value less than the threshold will considered as attacker and nodes with value greater than or equal to threshold is considered as trustable. The attacker nodes are avoided during the routing procedure. The behavior aspects to monitor the trust calculation are packet forwarding, network layer ACK, confidentiality, integrity, authentication, remaining energy. The trust value calculated by the following equation.

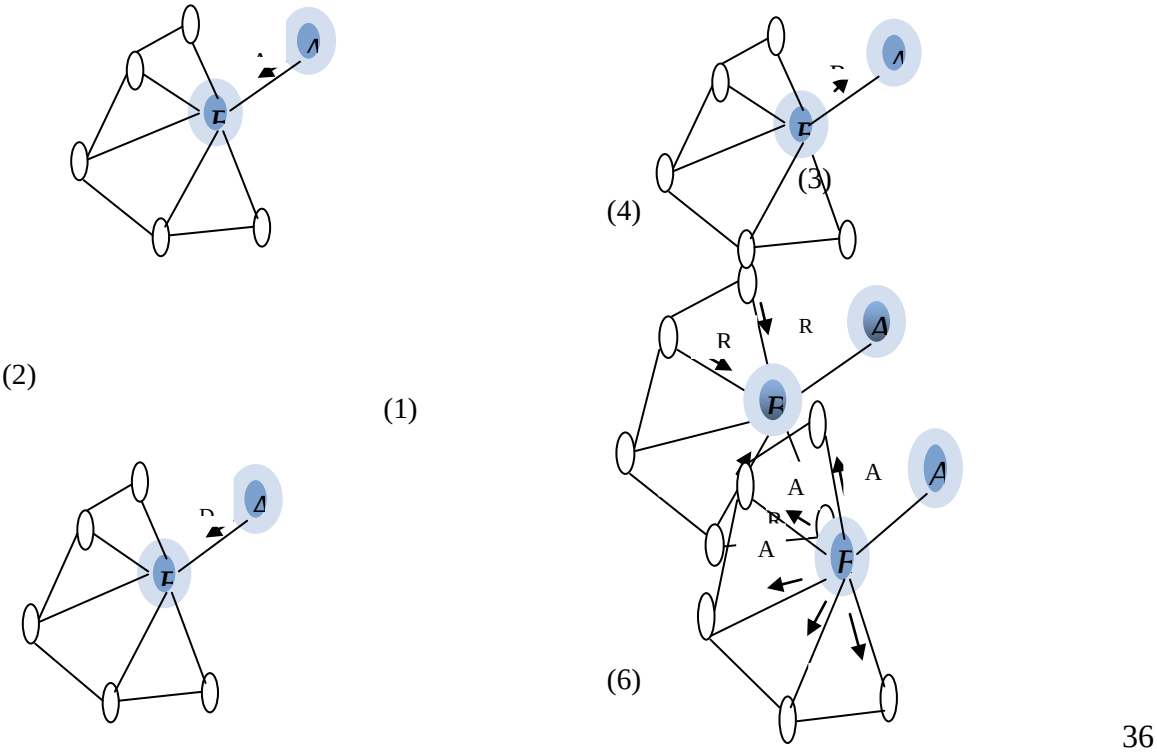
T = S /(S+F) (1)

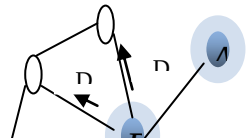
Where T denotes the trust value. S and F are the success and failed co-operations successively. To perform routing decisions, a weighted cost function is calculated which incorporates the trust information as well as the location information. The weighted function is as follows.

W (T)*T+W (D)*D (2)

Where W (T) and W (D) are the weights applied to the trust value and distance respectively and D is the distance. Using (2) calculates the trust value of each node. The nodes with trust value greater than the threshold will select. Then apply SPIN-PP protocol.

The protocol starts when a node advertises new data that it is willing to disseminate. It does this by sending an ADV message to its neighbors, naming the new data (ADV stage). Upon receiving an ADV, the neighboring node checks to see whether it has already received or requested the advertised data. If not, it responds by sending an REQ message and the trust value for the missing data back to the sender (REQ stage). The protocol completes when the initiator of the protocol responds to the REQ with a DATA message, to the node with the trust value greater than or equal to the threshold, containing the missing data (DATA stage). Figure 3 shows an example of the protocol. Upon receiving an ADV packet from node A, node B checks to see whether it possesses all of the advertised data (1). If not, node B sends an REQ message back to A, listing all of the data that it would like to acquire (2). When node A receives the REQ packet, it retrieves the requested data and sends it back to node B as a DATA message (3). Node B, in turn, sends ADV messages advertising the new data it received from node A to all of its neighbors (4). It does not send an advertisement back to node A, because it knows that node A already has the data. These nodes then send advertisements of the new data to all of their neighbors, and the protocol continues.





(5)

igure3. The trust based SPIN-PP protocol. Node A starts by advertising its data to node B (1). Node B responds by sending a request to node A (2).After receiving the requested data (3), node B then sends out advertisements to its neighbors (4), who in turn send requests and its trust value back to B (5), node B send its data to the nodes which trust value greater than or equal to the threshold (6).

Here, the node which does not contain the advertised data will send a REQ message along with the its trust value. Then the node B check all the neighbor's trust values (who are send the REQ message back to A). In the above example the node B send data to the neighbors with trust value greater than the threshold. The node B does not send its data to the attacker node (darkened node) because its trust value is less than the threshold.

If there is no such trust based SPIN-PP protocol ,the information send to the attacker node will refused to forward information to its neighbors and it will only cause overhead in the network .So, using this model we can avoid the attacker nodes from the information dissemination process.

IV. CONCLUSION

Previously, there is no available work on the integrated design of trust model and sensor protocol for information dissemination via negotiation for point to point communication. The main aim of trust based SPIN-PP is to provide security during information dissemination. In this, the trust model is used to find out the trust value of each node .Here each node's trust table contain only its own trust value. After finding the trust values of each node SPIN-PP is used for selecting the nodes for information dissemination. The nodes with trust value less than the threshold are refused to forward the information. These nodes are avoided from the routing procedure by checking its trust value in the trust table. An also the data reply contain a CRC field, which will provide integrity. So the trust based SPIN-PP provides more security in the case of routing attacks detection in wireless sensor networks.

REFERENCES

C. Giruka, M. Singhal, J. Royalty, S. Varanasi,"Security in wireless sensor networks", Wireless Communications Mob. Comput.2008; 8:1–24.

Chris Karl of David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Proc. of the IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113-127, May 2003

H. Li, M. Singhal, "A Secure Routing Protocol for Wireless ad hoc Networks", Proceedings of the 39th Hawaii International Conference on system Sciences, 2006.

Nathan Lewis, Noria Foukia, "Using Trust for Key Distribution and Route Selection in Wireless Sensor Networks" IEEE Globecom 2007, 26-30 Nov. 2007

Sapon Tanachaiwiwat, Pinalkumar Dave, Rohan Bhindwale, Ahmed Helmy "Location-centric Isolation of Misbehavior and Trust Routing in Energy-constrained Sensor Networks" IEEE

International Conference on Performance, Computing,
and Communications, 2004

A.A. Pirzada and C. McDonald, "Trust Establishment In Pure Ad-hoc Networks", Wireless Personal Communications Vol. 37, 2006, pp: 139– 163

Joanna kulik,Wendi heinzelman,Hari balakrishnan" Negotiation-Based Protocols for Disseminating Information in
Wireless Sensor Networks", Wireless Networks 8, 169–185,2002

Theodore Zahariadis, Panagiotis Trakadas , Sotiris Maniatis, Panagiotis Karkazis, Helen C. Leligou, Stamatis Voliotis," Efficient detection of routing attacks in Wireless Sensor Networks'"