Mobility Enabled Trustworthy Architecture for Wireless Sensor Networks

G. Mangalesh[1], S. T. Uma[2]

[1]M.E. Pervasive Computing Technology, Department of Computer Science,
Anna University (BIT Campus), Tiruchirappalli, TamilNadu, India.
gmangalesh@gmail.com

[2]Assistant Professor, Department of Computer Science
Anna University (BIT Campus), Tiruchirappalli, Tamilnadu, India.
uma_arunai.yahoo.com

Abstract: ***A Wireless sensor networks (WSNs) consist of small, lightweight wireless sensor nodes which are randomly deployed in large numbers to cooperatively monitor the physical or environmental conditions, such as pressure, humidity, temperature or pollutants. Ensuring security for the WSNs is a critical issue nowadays. Traditional security schemes cannot always be applied to WSN. Therefore, modeling concepts like trust and reputation is applied to gain a certain level of security and confidence among inter-operating nodes. Trust is calculated for a sensor node based on past interaction experiences given by neighbor nodes for assessing the reliability. It was also to measure the security property of a node (e.g. whether a node is malicious or not). Trustworthy Architecture for the WSNs provides the trusted communication among the sensor nodes, based on trust and reputation models. In this paper, mobile trust node was introduced to calculate the trust value for each and every sensor node in WSN and also analyzed the performance metrics of mobility enabled trustworthy architecture for WSN. This concept increase the lifetime of WSN by reducing communication overhead Performance analyses were carried out by using the Network Simulator (NS2).***

Keywords: WSN, Mobile Trust Node, Trustworthy Architecture

1. Introduction

Recently Wireless sensor networks (WSNs) are applied in several applications such as Environmental monitoring, land sliding detection, ocean navigation, underwater movements, industrial automation and control, military surveillance, health monitoring, and home applications, etc. For some of the applications security was very essential. In military based applications sensor motes are randomly deployed in the border areas to monitor the intruders and terrorists. In such environment the sensed data from the sensor nodes need to be well protected and hided from intruders to ensure security parameters as confidentiality and integrity. These sensor motes can be easily misused by intruders due to security lack. Since security was needed for such applications. The sensor motes can also be used to sense the environment to collect the data like temperature, pressure, humidity, nuclear acid pollutants, vibration, etc. Sensor nodes are randomly deployed in network environment to detect and send the events to the base station or the cluster head. Trust evaluation and its management of WSN in any networked environment are challenging issues. Trustworthy architectures consider initiation of trust and its establishment provides secure reliable communication in wireless networks. In general, Trust is the level of assurance or confidence in the sensor node or network of nodes. Nowadays the Trust management plays a major role in every network based application. The security is highly needed when the sensor nodes are randomly deployed in hostile and military environment. The trusted architecture of sensor networks was applied in various sensor network applications such as Military application, Bank application and Health monitoring applications. The rest of this paper is organized as follows: Section 2 describes related work. Section 3 contains definitions and description on representation of trust value. Section 4 proposes evaluation

of trust using Mobile Trust Node. Section 5 describes architecture design of Mobile Trust Node. Section 6 explains simulation-based analysis and evaluation of trustworthy architecture, respectively. Section 7 concludes this paper and suggests some future directions

2. Related Works

There is different number of trust management schemes were introduced recently to ensure the secure communication among sensor motes in WSNs. To the best of our knowledge, very few comprehensive trust management schemes (e.g., Group Based Trust Management Scheme (GTMS) [7], Reputation-based Framework for Sensor Networks (RFSN), Agent-based Trust and Reputation Management (ATRM) [10], GTMS evaluates the trust values of each sensor nodes individually in WSN and works on two topologies. In intragroup topology distributed trust management approach is used and intergroup topology centralized trust management approach is adopted. Trust management in WSNs and pervasive computing using Bayesian estimation was studied in [9]. Here the authors proposed a framework that evolves trust based on Bayesian formulation. Even it is expensive, it helps to resist the Sybil attacks. In Heuristic approach based trustworthy architecture for WSNs (HATWA) [2], Network monitoring node is introduced to calculate trust value for all other sensor nodes in WSN. Various security models based on security, reliability, mobility was referred. The traditional trust management schemes provide trustworthy architecture for WSN with static nodes. In this paper, we proposing mobility enabled trust management scheme. This scheme provides the trustworthy architecture for WSNs with mobile nodes. The

Mobile Trust Node (MTN) was introduced into trustworthy architecture to calculate the trust value for sensor nodes. The mobility of MTN was based on the various mobility models. Here we choose Random Way Point mobility model for movement of network monitoring node.

3. Trust definitions and Representation

Our proposed trustworthy architecture calculates the trust value based on direct or indirect observations. In this section we described definition of trust and its representation [3].

3.1 Definition

Trust is a major factor in any kind of network, social or computer networks. It becomes an important factor for members of the network to deal with uncertainty about the future actions of other member nodes [10]. Thus, the trust becomes important in distributed systems or internet transactions.

3.2 Representation

Generally the trust value of a node can be represented as numeric value within certain ranges. In our proposed Architecture the trust value is represented as decimal value ranges from 0 to 1. The overall trust of node is represented as trust state which can be further represented as trusted, distrust and uncertain states. The Trust value 1 states that the node was trusted in nature and the value 0 represent the node was in untrusted.

4 Evaluation of Trust using Mobile Trust Node

The trustworthy architecture works in two stages for trust evaluation in the network using the Mobile Trust Node.

- Trust calculation at the node level
- Trust calculation at the cluster/group level

4.1 Node level trust calculation

Consider a network of 10 nodes in clustered architecture. MTN is the Mobile Trust Node whose selection is made based upon the optimum energy level. All the sensor nodes in the network are randomly distributed in the terrain. Each node is assigned a node ID and the network communication is managed by a Mobile Trust Node for the issues such as security and mobility. At the node level, the trust value can be calculated by the past interaction of the node which is stored in the Mobile trust Node. If the node 3 wants to have a trusted communication with node 6, it will send the ID of node 6 to MTN. The MTN follows the prosed model and heuristic algorithm for estimating the trust value of the node. If node does not have the past interaction, the trust can be calculated by successful iterations. However, if there is no peer recommendation for the node, pre trust the node is taken into consideration. Every cluster has a MTN as shown in figure, which has more energy than the other nodes. There are more number of MTN was present in network to calculate a trust value.

4.2 Trust calculation for a Group/Cluster

The process of trust calculation of the group or cluster was based on number of MTN. In order to calculate the trust for the group or the cluster, the Mobile Trust Node requests the Member Node will evaluate the trust state of every node based on the trust state for each node in the group/cluster; the trust state for the cluster can be assigned. If more than 80% of the nodes are in trusted state, then the MTN will assign the trusted state to the group/cluster and hence network nodes ensure reliable communication.

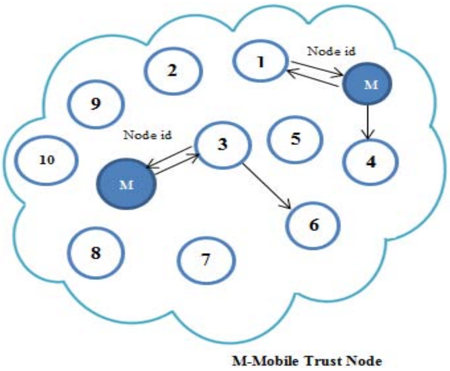

Figure 1. Trust value calculation of a node using Mobile Trust Node

5 Mobile Trust Node Architecture Design

1. A Mobile Trust Node in trustworthy architecture is more significant. Its architecture involves various stages. These stages are crucial due to their importance in selection of layer, routing protocol, and mobility model and energy consumption calculations.
2. OSI layer stage includes the various layers such as physical through application layer in which trust can be calculated based upon the fault management mechanism.
3. Routing protocol stage includes the selection of secure routing protocol such as AODV, LEACH, PEGASIS or SPIN. In this analysis AODV was selected as secured routing protocol.
4. Trust calculation is performed with mobility concerns. There are various kinds of mobility model such as Random way point mobility model, Group based mobility model, Manhattan mobility model. One of the Mobility model will be selected among the various mobility models. Here Random Way Point model was considered for various performance analyses.
5. Energy and power management is included for power and energy requirement for Trustworthy Architecture.

Algorithm for Security Model

```
Input: node ID.
Output: Trust state, secure communication.
Begin:
MTN checks authentication for M.N
If (M.N = = authorized) then
Allow communication
Else
Access abnegated
Exit
End if
M.N- Member Node
MTN –Mobile Trust Node
```

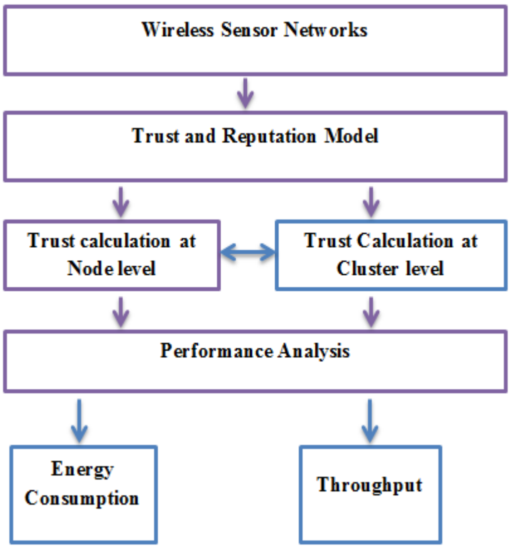
Wireless Sensor Networks
Trust and Reputation Model
Trust calculation at Node level
Trust Calculation at Cluster level
Performance Analysis
Energy Consumption
Throughput

Figure 2. Trustworthy Architecture Design

6 Simulation Specification

Network simulator 2(NS2) has been used for validating the sensor networks in terms of trust metrics. During simulation experiment, the rectangular, flat terrain dimension of 500 x 500m area in which sensor nodes are randomly deployed. The execution time can be assumed as 300s. The Random way point mobility model can be used by mobile node. Initially all ordinary nodes are assumed to be having 20 joules of energy. The Transmission ranges for all nodes can be 15m by default.

Table 1: Simulation specifications

Simulation Tool	*Network Simulator(Ns2)*
Terrain dimension	1000 x 1000m
Simulation time	300s
Routing Protocol	AODV
No of Member Nodes	10 20 30 40
No of Mobile Nodes	5
Mobility Model	Random way point Mobility Model
Transmission range	15m
Member Node energy	50joules
MTN Energy	100joules

Initially assume all the M.N having 20 Joules of energy. The energy of Mobile Trust Node was assumed to be 100Joules. For a Node level Trust calculation, Mobile Trust Node needs three packets. Performance metrics like throughput. Packet delivery ration of sensor network was evaluated by varying transmission ranges of the MTN. Performance of Mobility Enabled Trustworthy Architecture was analysed by increasing the number of MTN. The Mobile Trust Node consumes more energy than the other nodes. The MTN needs more energy because it should process all other nodes within the network.

6.1 Throughput

Total data traffic in kilobytes/sec successfully received and forwarded to the higher layer. Throughput shows protocol's successful deliveries for a time; the higher throughput shows better performance of the protocol. The following fig shows the throughput of Mobile Trust Nodes in mobility enabled Trustworthy architecture compared to static nodes.

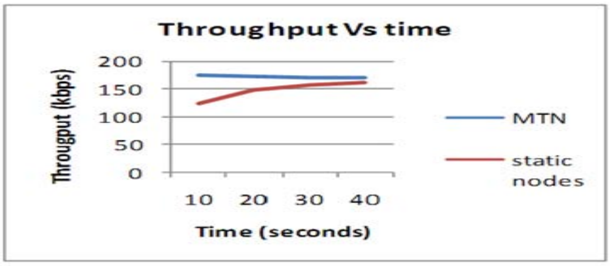

Figure 3. Throughput for Mobility enabled Trustworthy Architecture

6.2 Energy Consumption

Energy is major factor that includes in WSN. Here the energy remaining of sensor network by increasing number of nodes was analyzed and compared to existing Architecture.

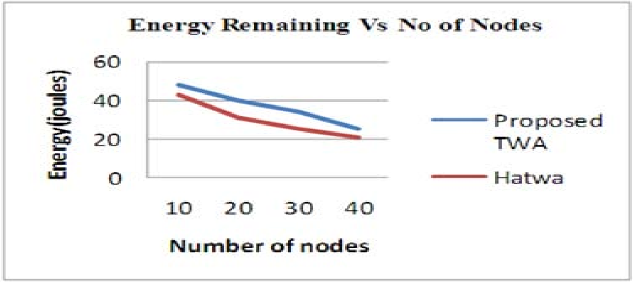

Figure 4. Remaining Energy of Sensor nodes

7. Conclusion

In this work, to solve the some security problems in WSN the Trustworthy Architecture was introduced. Trust calculation for node and cluster level was done. Performance of Mobility Enabled Trustworthy Architecture for WSN. In future, the lifetime of sensor networks has to be enhanced by selecting the secure energy aware routing protocol such as LEACH. The Simulation was carried out by using the Network Simulator.

References

[1] Akyildiz, Ian F., et al. "Wireless sensor networks: a survey." Computer networks 38.4 (2002): 393-422.

[2] Dhulipala, V. R. Sarma, N. Karthik, and R. M. Chandrasekaran. "A Novel Heuristic Approach Based Trust Worthy Architecture for Wireless Sensor Networks." Wireless Personal Communications (2012): 1-17.

[3] Gómez Mármol, Félix, and Gregorio Martínez Pérez. "Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems." Computer Standards & Interfaces 32.4 (2010): 185-196.

[4] Mármol, Félix Gómez, and Gregorio Martínez Pérez. "Trust and reputation models comparison." Internet Research 21.2 (2011): 138-153.
[5] Boukerch, A., L. Xu, and K. El-Khatib. "Trust-based security for wireless ad hoc and sensor networks." Computer Communications 30.11 (2007): 2413-2427.
[6] Zahariadis, Theodore, et al. "Trust management in wireless sensor networks."European Transactions on Telecommunications 21.4 (2010): 386-395.
[7] Shaikh, Riaz Ahmed, et al. "Group-based trust management scheme for clustered wireless sensor networks." Parallel and Distributed Systems, IEEE Transactions on 20.11 (2009): 1698-1712.
[8] Erman, Ayçegül Tüysüz, et al. "Enabling mobility in heterogeneous wireless sensor networks cooperating with UAVs for mission-critical management."Wireless Communications, IEEE 15.6 (2008): 38-46.
[9] Momani, Mohammad, Subhash Challa, and Rami Alhmouz. "Bayesian fusion algorithm for inferring trust in wireless sensor networks." Journal of Networks5.7 (2010): 815-822.
[10] Kumar, G., I. Titus, and Sony I. Thekkekara. "A Comprehensive Overview on Application of Trust and Reputation in Wireless Sensor Network." Procedia Engineering 38 (2012): 2903-2912.
[11] Reddy, Yenumula B. "TRUST-BASED APPROACH IN WIRELESS SENSOR NETWORKS USING AN AGENT TO EACH CLUSTER."

Author Profile

G. Mangalesh received the B.Tech (Information technology) degree in 2010 from Mepco Schlenk Engineering College, Sivakasi. He is currently doing M.E. (Pervasive Computing Technology) degree from Anna University (BIT Campus) Tiruchirappalli.

.