ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Isolated Industrial Surveillance Using Wireless Sensor Network with Trust Mechanism

S. Selvakumari,R.Parthiban

Department of CSE, Arunai College of Engineering, Tiruvannamalai, Tamilnadu, India

Department of CSE, Arunai College of Engineering, Tiruvannamalai, Tamilnadu, India

ABSTRACT— A wireless sensor networks (WSN) is a distributed self-directed sensor nodes to cooperatively monitor the physical and environmental conditions within their vicinity. Trust becomes more important for autonomous sensor nodes deployed in hostile and military environment. The trust in WSN poses greater challenges of the system and the challenges are reliability, security, mobility ,faultTolerance and other attributes of trust worthy system.This paper introduced a new approach for the validity of the trust management to achieve the full trust worthiness of the networks. So this paper solves the problems of security issues related to both clustered and layered architecture sensor network and provide the high fault tolerance functionality to the sensor nodes.

I. INTRODUCTION

Sensor network are highly distributed small, lightweight nodes in distributed network to monitor the physical and environmental conditions. Due to the wireless nature of the sensor networks, nodes become open for various attacks during communication. Developing the secure network between the nodes of sensor networks is challenging compared to traditional networking methods due to resource constraints problems. Sensor networks found themselves more important in the field of restricted environments and unattended environments. So it is imperative to provide few security policies and other reliable services in terms of trust management to safeguard the sensor network application environment. In this regard, trust becomes critical issue in self-configurable, dynamic and autonomous sensor networks. The wireless radio communication nature raises the possibility of attacks and risks.Security plays an important role in the sensors deployed in the hostile environments. The sensed data must be protected to ensure the confidentiality. Security requirements of sensor networks are very similar with those of conventional networks; the applicable security solutions are quite different due to their specific characteristics. First, sensor networks are highly application-oriented and as such various applications bring diverse security needs. Thus, there is a clear need to adapt security services when applications change. Second, the sensor nodes usually have limited communication bandwidth, CPU, memory, and especially the battery capacity. In unattended environments, the sensor nodes are prone to attacks ranging from simple physical attacks to convoluted analysis. The resource constrained sensor nodes are easy to attack and hard to protect from the hackers. So constructing the trust management for the wireless sensor networks is very important.

Trust is an old but important issue in any networked environment and can solve some problems beyond the power of the traditional cryptographic security. Trust and trust establishment between nodes in WSNs are the initial point for constructing the network.

In literature, the trust is the level of confidence in a person or thing. Trust in networks is the degree of belief or confidence about the other nodes based on the past interaction and observation. Trust in wireless sensor networks may be defined as, "A combined characteristic model in WSN for providing reliability, security with respect to mobility". Trust management solves the problem of access control, providing reliable routing path and security mechanisms. The properties of the trust are cooperativeness, subjectivity, semi-transitivity, temporalness, dynamicity, and non-monotonicity.

ORGANIZATION OF THE PAPER:

The remainder of this paper is organized as follows, in section2, we have the related works. Section3 have an security issues in WSN and algorithm used. Section4

Trust Calculation using Direct Trust. Section5 concludes the paper.

II. RELATED WORKS

Bayesian network Trust Model for Wireless Sensor Networks [12] (BNWSN) introduces a new trust model called Bayesian trust model to combine more than one trust component. Here the model combines communication and data trust to produce the overall trust. The model is robust and generic which allows the components to be added or removed easily form the model. Bayesian network represents a probabilistic framework with Bayes rule for representing computational feasibility. The Bayesian network consists of a set of random variables and set of edges. The variables are used to represents the nodes and directed edges represent the arcs between the variables. Normal distribution is used to calculate the data trust and beta distribution is used to calculate the communication trust. The resulting third distribution is the multiplication of beta and normal distributions. The several simulations are conducted in the self-written simulator for verifying the total trust of the network includes the data and communication trust.

In Trust Model using Fuzzy Logic, Authors introduced the explicit trust to sensors to allow them to reason with trust and to make the decision with concerning other nodes. They suggested a trust model with fuzzy logic in the wireless sensor networks to distinguish the normal and faulty or malicious nodes. The algorithm used here consists of three steps: fuzzy matching, inference and combination. Fuzzy if then rules are applied here to take the decision for communication with other sensor node. Trust is an aggregation of past interactions among the sensor nodes in the network. The model is applied to the sensor network to show how the trust mechanisms are involved in communicating algorithm to choose the path from source to destination. The model is used to differentiate the normal sensor node and malicious or faulty node. The malicious node can attack and contaminate the network. The proposed fuzzy model uses the concepts of trust, mistrust and distrust introduced in [11]. This model used MATLAB for implementation. They recursively applied the numerical formula to calculate the average value for path from source to destination. Then they used the fuzzy logic to choose the correct path from source to destination.

In Group based Trust Management Scheme (GTMS), author proposed a new light weight trust management scheme for wireless sensor networks. It works with two different topologies: intragroup and intergroup topologies, where distributed trust management and centralized trust management is adopted respectively. For the intragroup network, each node in the network calculates the individual trust values for all group nodes in the cluster. Based on the trust values, a node can assign any one of the possible states to the node in the cluster. The possible states are Trusted, Untrusted and Uncertain. Based on the trust states of the node in the cluster, the cluster head will assign the overall trust state for the group and also detects the malicious and faulty nodes. The clustering scheme and group deployments enable the sensor node to work in cooperative manner. So the selection of cluster head and the detection of faulty or malicious nodes are easy. It evaluates the trust for the group of nodes rather than a single node in the cluster. It also needs less memory,energy consumption and communication overhead when compared to other schemes. GTMS is a mechanism to detect the malicious and faulty nodes and also provides some degree of prevention mechanism. The authors showed the simulation using Sensor Network Simulator and Emulator (SENSE) by considering the static nodes organized in grid fashion. The simulation results indicated that the proposed scheme having less computation and low memory overhead.

III. SECURITY ISSUES IN WSN

Sensor network are more vulnerable to attack due to it’s open environment. Various security issues that are related to sensor nodes are

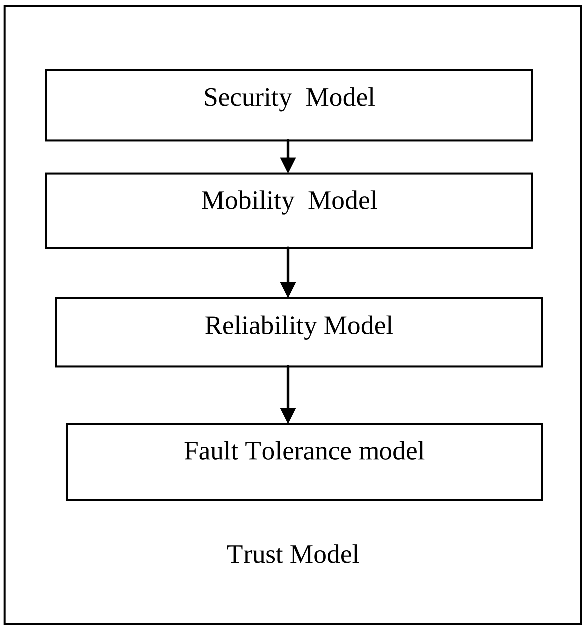
- The Sybil attack
- A selective feedback attack
- Sinkhole attack
- Wormhole attack
- Hello flood attack

To overcome the above attacks we are proposing an protocol called Localized encryption and Authentication protocol, INSENS, security protocol for sensor network(SPINS)

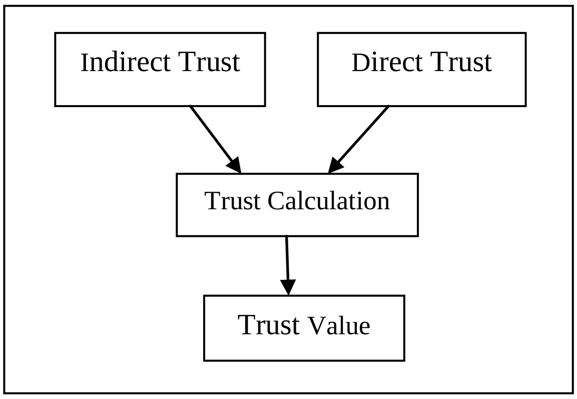
IV.TRUST CALCULATION USING DIRECT TRUST

A.TRUST MODEL

The value of the trust in WSN depends on the security attribute, mobility attribute, reliability attribute and fault tolerance of the node as in model .The security model of the node in the trust framework involves the use of secure routing protocol and encryption of packets for routing. The value of the trust in the security model is high, when it uses the secure routing protocol and encryption technique. Otherwise the trust value of the node in security model is zero. The mobility model of the node in the trust framework involves the use of secured mobility model for the node. The secured mobility model and the minimum energy consumption during the mobility ensure the high trust value in the mobility model of the node. Otherwise the trust value of the node in the mobility model is zero. The trust value in reliability model of the node is high when it uses the data fusion of the packets with less energy consumption. The trust value in fault tolerance model of the node is high when it provide the less message overhead,less computation time and high network lifetime.



The trust value of the node can be calculated in two steps as shown in the figure. First step involves the calculation of the trust value of the node by the past interactions and the recommendations by the neighbors in the networks. This evaluation of the trust value is called indirect trust value of the node. The indirect trust value is also called as initial trust value of the node. If the initial trust value of the node is adequate for communication then the node starts its communication. Otherwise it goes for direct value trust calculation.



Four models as in the trust framework: security model of the node, mobility model of the node, reliability model of the node and fault tolerance model. The node evaluates the trust value for every model of the node.
If the trust value in the security model is adequate then it starts the communication.

Trust can be calculated by having the following modules.

1. Security model
2. Reliability model
3. Mobility model
4. Fault Tolerance model

Otherwise it starts to evaluate the trust value for the mobility model. If value in the mobility model is inadequate for communication then it starts the evaluation for the reliability model of the node. If the reliability model of the node is inadequate for communication then it starts the evaluation for the fault tolerance model of the node. If fault tolerance model then the node calculates the total trust by adding the indirect trust and direct trust. If the total trust value of the node is not enough for the trusted communication then the node denies the communication request of the node.

1) SECURITY MODEL

Security is essential to the success of WSN applications, especially for those mission-critical applications working in unattended and even hostile environments. Providing satisfactory security protection in WSNs has ever been a challenging task due to various network & resource constraints and malicious attacks.

In security model, we address the node authentication to provide the access control. Encryption of packets covers the data security in sensor nodes. The secure and anonymous routing provides communication security in the network. The trust value for the security model of the node is high if node has secure routing protocol, access control and encryption of the routed packets. The following algorithm was proved good in our computer simulation experiments for the high trust value in the security model of the node in the network.

Security mechanisms such as encryption and authentication are essential to protect information transfer between sensor nodes deployed in hostile environments. Due to the radio broadcast and ad-hoc property and the highly resource-constrained sensor nodes within sensor networks,implementing security mechanisms in an efficient way without sacrificing the strength of their security properties is a major challenge for sensor network security.

The key aspects in security model are encryption, authentication, secure and anonymous routing.

```
Input:  ID, Signal strength.
Output: Trusted, Secure communication using HATWA
Initial Condition: Select CM, C. N entering into terrain.
begin:
    CM checks authentication.
    C.N Exchange key with CM
    if(C.N == authorized)then
    allow communication
    else access abnegated exit
        Select secure routing protocol.
    Encrypt the data using encryption algorithm
    and route the packets.
    if(C.N==mobile) then
    select mobility model
    else C.N= static
    Calculate hop count, delay, and packet loss.
```

trust value for the node in the reliability model, if it has less acquisition delay, latency and energy consumption.
The key aspects in reliability model are data fusion and latency.

PSEUDO CODE FOR RELIABILITY MODEL

```
Input: C.N
Output: reliable communication, latency, acquisition delay, energy consumption.
Initial condition:
        CM permits C.N, Authorized C.N
undergoing communication
Begin:
        If (C.N undergone communication) then
        Calculate latency, bandwidth, and energy
        consumption
        endif.
        If (C.N receives packets) then
        Calculate acquisition delay, energy
        consumption during reception of the
        packets.
        endif.
        If (V.N sends packets) then
        Calculate energy consumption during the
        transmission of the packets.
End.
```

2) MOBILITY MODEL

PSEUDO CODE FOR MOBILITY MODEL

Mobility is defined as movement of nodes in wireless sensor networks. The mobility model is designed to describe the movement pattern and the location of the node. In mobility model, the localization issue helps us to locate the nodes in the terrain. We can estimate the mobility of the node based on the destination and source node location. Mobility helps to propagate the trust between the nodes. The trust aggregation can be improved by the mobility of the node.
Various mobility models in WSN are Random Waypoint model, Reference Point Group Mobility, Freeway (FW) Mobility Model and Manhattan Mobility (MH) Model. Secured mobility model and optimum energy consumption ensures trust worthiness in the ad hoc network environment. The trust value in the mobility model of the node is calculated based on the optimum energy consumption during mobility of the node and the selection of the mobility model based on the application requirement.

```
Input: C.N
Output: hop count, spot of nodes, energy consumption.
Initial condition: authorized C.N undergoing secure
communication.
Begin:
        If (C.N==mobile)
        Select mobility model, Estimate mobility:
calculate hop count.
        Estimate localization: calculate spot of nodes
        and energy consumption.
        Else (C.N= static)
        Calculate energy consumption of node during
the mobility.
        endif
End.
```

3) FAULT TOLERANCE MODEL

Fault tolerance provides WSN with reliable connection and dissemination of data, preserving limited resource and power energy in sensor network. Nodes can withstand to perform the process even when the failure occurred in the data. Fault tolerance in WSN has three phases fault models, fault detection ,identification and resiliency mechanism at four level of abstractions like hardware, system software, middleware and application. Application of Fault tolerance used in node placement, topology control, target and event detection, data aggregation and gathering, sensor surveillance. various algorithm are used to provide fault tolerance like Fast Fault Tolerance Partitioning Algorithm for WSN, Adaptive algorithm, Heterogeneous fault tolerance, Discrepancy minimization based fault detection correction technique.

Fast Fault Tolerance Partitioning Algorithm provide a random uniform distribution of sensor nodes to find the maximum number of partition of the nodes so each partition is connected and cover the many nodes in the network.

PSEUDO CODE FOR FAULT TOLERANCE MODEL

```
Input: C.N ID
Output: Reliable communication, Network Lifetime,
computation  time, message overhead, Diameter of
Partition.
Initial Condition: CM Permits CN,CN undergoing
communication
begin:
    if(C.N == failed)then
    Reconstruct the affected partition
    Endif
    if(C.N==Not failed) then
    Calculate the performance attributes.
    Endif
End
```

V. CONCLUSIONS

We have introduced the trust mechanism for controlling the industry appliance unit remotely with algorithm and trust models for the key issues in the wireless sensor network. The design of the trust mechanism in WSN must be taken into a account with diverse need including reliability and security. The proposed trust mechanism of trust may be integrated into many other real applications

REFERENCES

[1] *Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d'Auriol,Heejo, Sungyoung Lee, and Young-Jae Song, " Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks", IEEE transactions on parallel and distributed systems, VOL. 20, NO. 11, NOVEMBER 2009*

[2] *N.Karthik, V.R.Sarma Dhulipala, "Trust Calculation in Wireless Sensor Networks", IEEE International conference on Communication, Electronics and Technology, ICECT'11.*

[3] *3.I.F.Akyildiz, W. Su, Y. Sankarasubrarnanian, and E. Cayirci, "Wireless sensor networks: A survey," Computer Networks, Elsevier Science, 38(4), pp. 393-422, 2002.*

[4] *Tae Kyung Kim, and Hee Suk Seo, "A Trust Model using Fuzzy Logic in Wireless Sensor Network", World academy of science and engineering and Technology- 42, 2008.*

[5] *5.V.R.SarmaDulipala,N.Karthik,R.M.Chandrasekaran,"A Novel Heuristic Apporach Based Trust Worthy Architecture for Wireless Sensor Neiworks",Wireless Personal communications.*

[6] *6. M. Momani, S. Challa and R. Alhmouz, "BNWSN: Bayesian Network Trust Model for Wireless Sensor Networks", in Mosharaka International Conference on Communications, Computers and Applications (MIC-CCA '08), Amman, Jordan, 2008*