Enhance Security in Wireless Sensor Network Using Trust Awareness Routing Protocol (TARP)

Kanhaiya Jee Jha[1], Gayatri Pandi[2]

[1]Research Scholar, Computer Engineering Department, L.J College of Engineering & Technology, Gujarat, India
[2] Assistant Professor ,Computer Engineering Department, L.J College of Engineering & Technology, Gujarat, India

ABSTRACT

As the Trust issue in wireless sensor network is emerging as an important factor in security of node. Sensor networks are implementing on large scale in real time environments due to its incredible uses in real life. Wireless sensor network (WSN) don't need human interference for its working so they can place where human cannot reach easily. It is necessary to analyze how to resist attack with a trust scheme. In this report we categorize various types of attacks and counter measures related to trust schemes in WSNs. Furthermore we provide the development of trust mechanism which give a short stigmatization of classic trust methodologies and emphasize the challenge of soft trust scheme in WSNs. Based on the analysis of attack and the existing research an open field and future direction with trust mechanisms in WSNs is provided. In this paper Design efficient wireless sensor network with efficient node selection using PSO with Trust Mechanism for improving the efficiency of existing system. Wireless sensor networks are mainly deployed to monitor events and report data, both continuous and discrete the development of new trust models addressing the continuous data issue and also to combine the data trust and the communication trust to infer the total trust.

Keywords: *Wireless sensors network, Security, Energy efficient, Trust, Communication trust, Data trust, Recommendation trust, optimal route, PSO algo. , Trust management.*

1. INTRODUCTION:

WSNs are emerging technologies that have been widely used in many applications such as emergency response, healthcare monitoring, battlefield surveillance, habitat monitoring, traffic management, smart power grid, etc. However, the wireless and resource-constraint nature of a sensor network makes it an ideal medium for malicious attackers to intrude the system. Thus, providing security is extremely important for the safe application of WSNs.

Wireless sensor networks is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical and environmental condition. Critical vulnerabilities such as node capture and Denial-of-service (DoS) attacks. Various security mechanisms, e.g., cryptography, authentication, confidentiality, and message integrity, have been proposed to reduce the security threats such as eavesdropping, message reply, and fabrications of messages.

Sensor nodes are small in size and able to sense events, process data, and communicate with each other to transfer information to the interested users. Typically, a sensor node consist of four sub-systems:-

- Computing sub-system (processor and memory).[1]

- Communication sub-system (transceiver).
- Sensing sub-system (sensor).
- Power supply sub-system (battery).

WSNs are a collection of self-organized sensor nodes that form a temporary network. In wireless sensor network, trust specifies the reliability or trust worthiness of sensor node. In this system, trust model specifies & plays an important role in identifying misbehavior nodes and providing collaboration among trustworthy nodes. The reputation –based framework for high integrity sensor network was first trust based model designed and developed for sensor networks.
Trust is defined as a belief level that one sensor node puts on another node for a specific action according to previous observation of behaviors. Trust value ranges from 0 to 1 where 1 is completely trustworthy. Trust are of mainly three types, they are as:-

- Direct Trust: based on direct communication behaviors.
- Recommendation Trust: filtered recommendations for 1-hop nodes.
- Indirect trust: trust for multi-hop nodes based on recommendations.

Trust has numbers of different properties, they are as following: - [1]

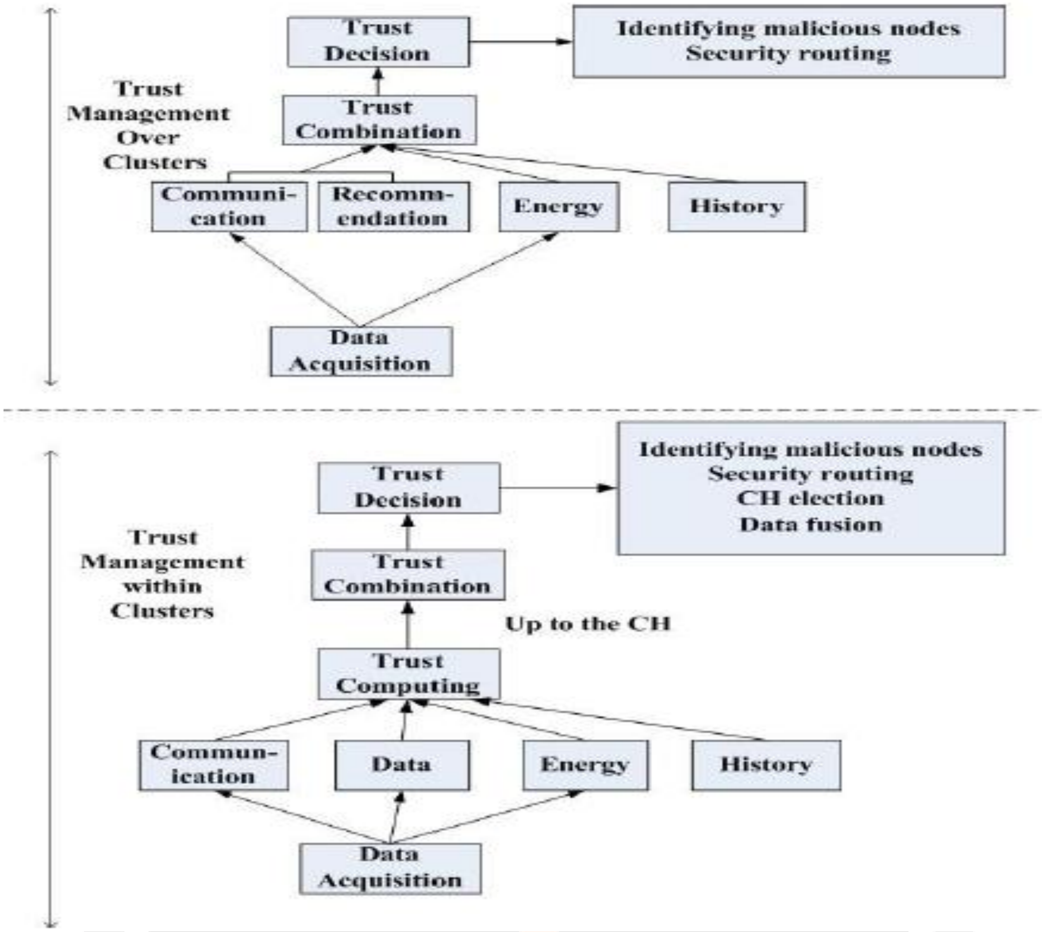
- Asymmetry: If node A trusts B, it does not imply nodes B trusts Node A.
- Transitivity: Trust value can be passed along a path of trusted nodes. If node A trust Node B and node B trust node C, then A trust C at certain levels. It is important in trust calculation between two non–neighbor nodes.
- Composability: Trust values received from multiple available paths can be composed to obtain an integrated value

2. RELATED WORK:

Now a days lots of research is going on WSN as it is a new system of technology which is used in lots of field. This technology helps us in numbers of different field it also makes our work very easy. Main factor is of keeping the data's more secure it can be done by using different mechanism, one of the mechanism is Trust Mechanism. We have Analysis and summary of the different papers. All papers points are mentioned and shows the things which is included and to what more importance is given, and what more should be done in future.

2.1 A Hierarchical Trust Model for Cluster-based Wireless Sensor Network. [2]

A hierarchical trust model for cluster-based wireless sensor network is proposed. According to the differences between cluster heads and general nodes, the distributed and centralized trust management mechanisms are combined in this paper.
In this model, the computation of node trust is based on communication, data and energy aspects. The defined trust value can denote the trust level of WSN nodes objectively and respond to a variety of security threats which wireless sensor network might encounter.



.

Fig-1 Framework for trust model [1]

A hierarchical dynamic trust management model is proposed for cluster-based wireless sensor network, which is based on three trustworthiness aspects such as communication, data and energy.

The trust model is featured with distributed and centralized trust management framework, the structure difference within one cluster and over clusters, and the different missions. The model has a good performance in dynamic adaptability, fault tolerance and superiority.

2.2 Improving Security in Wireless Sensor Network Using Trust and Metaheuristic Algorithms. [2]

Trust is important in wireless networks as collaboration /cooperation among nodes is critical to achieving system goals like routing reliability which is NP Hard. In this work a trust based Cluster Head selection mechanism using Firefly based Metaheuristic is proposed to improve the security and network lifetime of the WSN.

In this work the proposed algorithm was: - [3]

- Implemented in a mote test bed consisting of 23 motes and one laptop acting as the base station.
- Simulations were carried out extensively using MATLAB and varying the number of nodes from 100 to 900.

Each node will calculate trust for all its surrounding nodes and store these values locally for later usage. [4]

$$A = \mp \sum_{i=1}^{n} T_{y_i}(x)$$

$$B = \frac{\sum_{y=1}^{m} T_y(x)}{m}$$

The proposed Trust Firefly Algorithm decreased the end to end delay when compared to Weighted Clustering Algorithm. The packet delivery ratio is significantly improved for the proposed Trust Firefly Algorithm compared to Weighted Clustering Algorithm. The average Packet Delivery Ratio (PDR) improvement of the proposed system was 33.12%.

2.3 An Efficient Distributed Trust Model for Wireless Sensor Networks. [5]

In this paper, The Authors proposed an Efficient Distributed Trust Model (EDTM) for WSNs. First, according to the number of packets received by sensor nodes, direct trust and recommendation trust are selectively calculated. Then, communication trust, energy trust and data trust are considered during the calculation of direct trust.

TRUST CALCULATION IN EDTM

1. The calculation of Direct Trust

1.1 Calculation of the Communication Trust

Tcom = 2b + u/2

1.2 Calculation of the Energy Trust [5]

$$T_{ene} = \begin{cases} 1 - p_{ene}, if E_{res} \geq \theta \\ 0, else \end{cases}$$

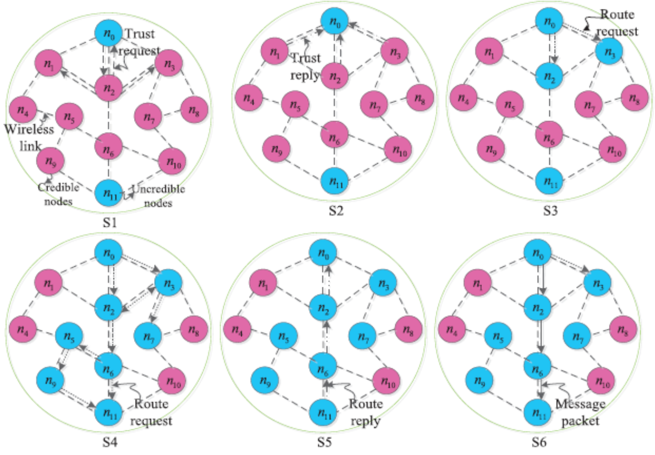
A distributed and efficient trust model named (EDTM) is proposed. During the EDTM, the calculation of direct trust, recommendation trust and indirect trust are discussed. Furthermore, the trust propagation and update are studied. Simulation results show that EDTM is an efficient and attack-resistant trust model.

2.4 Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network [6]

The typical network attacks caused by the limited energy and the poor deployment environment of wireless sensor network on data transmission, a trust sensing-based secure routing mechanism (TSSRM) with the lightweight characteristics and the ability to resist many common attacks simultaneously is proposed in this paper.

Here the process is divided into main 3 parts: - [6]

- ◦ NETWORK INITIALIZATION PROCESS
- ◦ ROUTE CONSTRUCTION PROCESS
- ◦ ROUTE MAINTENANCE METHODS



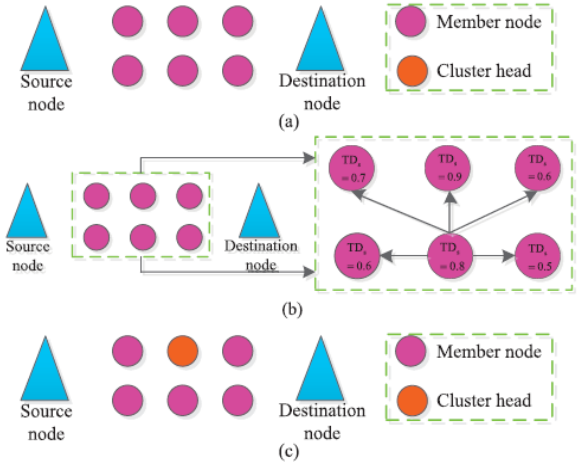


FIG-2 ROUTING PROCESS [6]

FIG-3 CHOICE PROCESS OF CLUSTER HEAD [6]

This paper presents a trust sensing based secure routing mechanism to handle common network attacks. An optimized routing algorithm is proposed by using semiring theory, which considers the trust degree and other QoS metrics.

2.5 Communication and Data Trust for Wireless Sensor Networks using D-S Theory. [7]

In this paper, a trust mechanism which evaluates Communication trust and Data trust for WSNs. Communication trust is computed from direct and indirect observations of the neighbour's forwarding behaviour. Direct trust is derived from the consistency of forwarding behaviour. Author used Weighted Dempster-Shaffer (D-S) theory to compute indirect trust. Data trust is computed by using median of sensor data.

- Direct Trust (DT^B_A (t)): [7]

$$DT_A^B(t) = DT_A^B(t-1) \times cos(\frac{\pi}{2} \times \delta_t)$$

- Indirect Trust (IT^B_A (t)): [8]

$$IT_A^B = m_x^B(H) \bigoplus m_y^B(H) ... \bigoplus m_y^B(H)$$

The proposed model TWSN uses weighted Dempster-Shaffer theory to aggregate the recommendations. Direct trust is computed using forwarding ratio with cos(x) function to mitigate on-off attacks. TWSN mitigates packet modification/dropping attack, bad mouthing attack, collusion attack and on-off attack. We also derive data trust to identify malicious sensor data.

3. PROPOSED METHODOLOGY:

The proposed Trust model flow chart consist of numbers of step. In this mainly there is three steps in which consist creation of network ID and object ID and next to it the calculation of neighbor and Trust value come into picture which will show the most trustworthiness using the PSO Algo. This Algo. Will help in getting optimized Route and after getting optimize route the data is transmitted with more security and through proper node using the shortest or best applicable path. We will discuss the step one by one.

3.1 Create Network Topology: -

This is the 1st step of the proposed method. In this step the Network topology is created which is used in connecting the numbers of nodes together or making a bridge among the different nodes.

3.2 Create Network ID & Object ID: -

This is the 2nd step which includes the creation of network ID and object ID. In this step ID is created for network and object. This is done for the Identification purpose. Which further helps during the node connection and in getting the proper path.

3.3 Calculation of neighbor and Trust Value: -

This is the step which consist of calculation of neighbor and trust value. Both can be calculated using different methods like calculation of communication trust, Energy trust, Data trust, Recommendation trust, Recommendation reliability, Indirect trust etc.

3.4 PSO Algo: -

This is the step in which PSO Algo is used for getting optimized Route. This is the algo used in this proposed methodology which gives us a short and best applicable path.

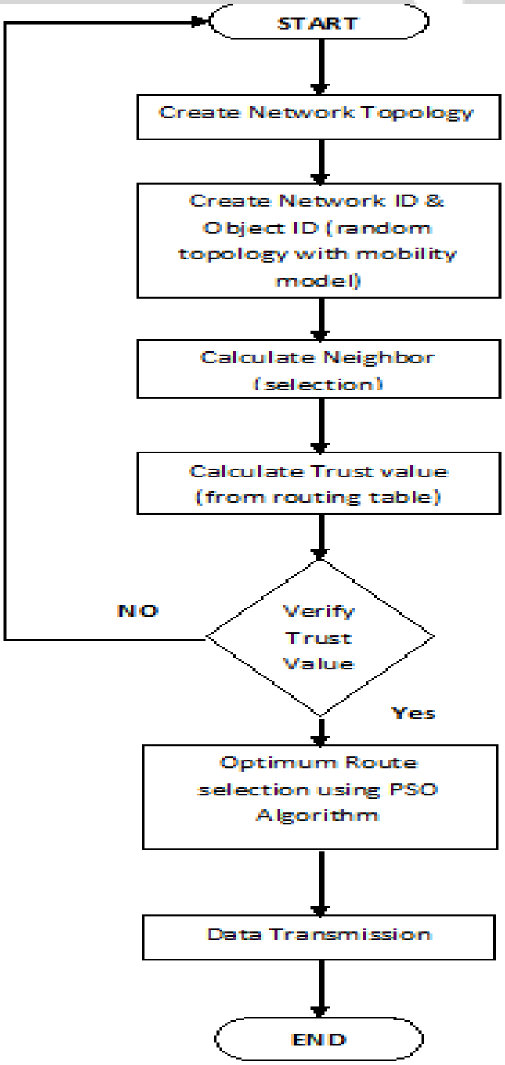

START
Create Network Topology
Create Network ID & Object ID (random topology with mobility model)
Calculate Neighbor (selection)
Calculate Trust value (from routing table)
NO
Verify Trust Value
Yes
Optimum Route selection using PSO Algorithm
Data Transmission
END

FIG -4 PROPOSED CHART

4. CONCLUSION:

In all papers we have seen that any one theory is taken and one process is fallowed for e.g. distributed and centralized trust management framework, Trust Firefly algo. , semiring theory etc. is used. We here use a proposed method which will give more security and less use of energy, load balancing process is fallowed as well as trustable node selection and optimum node selection process is made easy and more accuracy is obtained using the calculation of neighbor and trust value and also using PSO algo.

5. REFERENCES:

1. Li Ma ,Guangjie Liu *"*A Hierarchical Trust Model for Cluster-based Wireless Sensor Network*"*978-1-4799-9892-0/15 ©2015 IEEE.

2. L. Moraru, P. Leone, S. Nikoletseas, and J. D. P. Rolim, "Near optimal geographic routing with obstacle avoidance in wireless sensor networks by fast-converging trust-based algorithms, " in Proc. 2007 ACM Workshop QoS Security Wireless Mobile Netw., pp. 31–38.

3. Xianji Jina , Jianquan Liang b,Weiming Tonga , Lei Lua , Zhongwei Li "Multi-agent trust-based intrusion detection scheme for wireless sensor networks" 0045-7906/© 2017

4. Khan, Muhammad Khurram, Yang Xiang, Shi-Jinn Horng, and Hsiao-Hwa Chen. "Trust, security, and privacy in next-generation wireless sensor networks."International Journal of Distributed Sensor Networks (2013), pp: 1-2

5. Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu, and Mohsen Guizani "An Efficient Distributed Trust Model for Wireless Sensor Networks" 1045-9219 (c) 2013 IEEE.

6. G. Han, J. Jiang, L. Shu, J. Niu and H.C. Chao, "Managements and applications of trust in Wireless Sensor Networks: A Survey". Journal of Computer and System Sciences, pp. 1-16, 2013

7. Wanlei Zhou PingLi Yanli Yu, KeqiuLi. "Trust mechanisms in wireless sensor networks:attack analysis and countermeasures"35:867–880, 2012

8. Yick, Jennifer, Biswanath Mukherjee, and Dipak Ghosal "Improving Security In Wireless Sensor Network Using Trust And Metaheuristic Algorithms" 978-1-5090-2549-7/16/©2016 IEEE.