International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064

Review of Trust based Methodologies in WSNs

Satwant Singh[1], Usvir Kaur[2]

[1]Research Scholar, SGGSWU Fatehgarh Sahib, India

[2]Assistant Professor, SGGSWU Fatehgarh Sahib, India

Abstract: ***In this research paper we have done objective study on latest trust based methodologies that are used in securing the WSN, the focuses in our current study have been on the aspect of energy and memory consumption due to implementation of trust based techniques. We have developed a comparative chart and review of the techniques and have found certain limitations worthwhile for conducting this research work with respect to previous work. Based on these limitations we have also recommended certain valid points to improve trust based methodologies.***

Keywords: Wireless Sensor Networks, Trust Based Methodologies, Energy consumption patterns, NBBTE Algorithm

1. Introduction

A sensor network is an infrastructure comprised of nodes capable of sensing, computing and communication elements. The various basic components in a wireless sensor network are an assembly of distributed or localized sensors, an interconnecting network, a central point of information clustering and a set of computing resources. The main components of WSN are sensor nodes and base station. Sensor nodes are very small with hardware equipped with microcontroller, transceivers and battery [1].

Wireless sensor networks (WSNs) have been implemented in battlefield, hospital, forest and other crucial fields. Various attacks with the principles in computer networks pose threats to WSNs. WSNs consist of battery-operated sensor devices with computing, data processing, and communicating components. The ways the sensors are deployed can either be in a controlled environment where monitoring and surveillance are critical. In the uncontrolled environments, security for sensor networks becomes extremely critical [6].

Trust management is the most important aspect of security in Wireless Sensor networks. A trust aware routing protocol is a routing protocol in which a node incorporates in the routing decision its opinion about the behavior of a candidate router. This opinion is quantified and called the trust metric. Trust metric should reflect how much a router is expected to behave, for example, forward a packet when it receives it from a previous node [2].

2. Related Work

- **Bayesian trust model*:*** Bayesian Trust methodology been used in research work [7] [11] to detect the selfish nodes. There are two different directions mentioned subjective and object trust. Trust calculation depends upon the node's behavior which stores the value. Bayesian methodology utilizes the prior probability of an event, which is then updated based on relevant evidences [4].
- **Game theory trust model:** Game theory model tries to capture the behaviour of nodes mathematically in situations where the decisions depend upon the behaviour of the other nodes. Trust mechanism based on game theory has been implemented to detect the selfish nodes [5].
- **Entropy trust model**: The concept of thermodynamics is used where entropy deals with how much uncertainty is there in a signal or event. [7] proposed a method for trust evaluation in Ad hoc networks which uses Bayesian model and entropy model.
- **Fuzzy trust model**: IF-THEN rules are used to solve any problem in fuzzy logic. The logic steps followed in fuzzy modes are fuzzy sets and criteria have to be predefined and input variables are initialized and fuzzy rules are applied to input data to obtain output. Finally the results are calculated and feedbacks are obtained.

3. Comparative View of Various Trust Based Methodologies in WSNs

Methodology	*Features*	*Disadvantages*
Bayesian trust model	1. In this system a framework has been developed using Bayesian formulation specifically beta reputation system, reputation representation, updates and integration. 2. The method employs watch-dog mechanism to calculate the reputation. 3. Once the packet was passed to other nodes, each node eavesdrop the packet whether it reaches the destination and formulates the trust value based on reputation scheme.	The main disadvantage is that trust evaluation is based only on node's QOS property and flat wireless sensor network architecture followed which may not be scalable.
Game theory trust model	1. Afrand et al based on cooperative game theory proposed a game between a sensor node and three factors namely cooperation, reputation and quality of security. 2. Cooperation between nodes means there is more reliable data communication between nodes and moreover node cooperates its reputation increases and misbehavior is easily detected. By combining these factors the trust value is calculated.	The main disadvantage of this scheme is its complexity, which makes it hard to implement.
Entropy based trust model	1. Sun yl et al proposed a trust model to detect selfish nodes and malicious modes. 2. It represents a framework to measure trust, trust propagation model and defend trust evaluation against attacks. 3. Possible attacks against the proposed system has been identified (Sybil attack) and various remedial techniques been applied.	This technique is used only for each attack individually. Therefore it does not show the joint effect of various attacks.

	4. This system improves the routing techniques and improves the throughput of network. It uses both entropy model and Bayesian model.	
Fuzzy trust model	1. Azzedine Boukerche et al proposed a trust system for pervasive and ubiquitous computing. 2. Malicious nodes are major threat in the networks and this problem is dealt using a security system based on trust management involves developing a trust model ,assigning credentials to nodes, updating private keys and managing the trust values of individual node. 3. Through this system a formal security analysis of trust system is proposed and malicious nodes are detained from pervasive and ubiquitous computing	There is again the problem of memory overhead. Inefficiency of lot of if-else rules.

4. Major Issues in Trust Management in WSNs

The various research issues includes [3] Biological applications- Biological Task mapping, Biomedical signal monitoring. In Commercial applications includes – Smart parking, Event Detection, Structural Health Monitoring. The various resources constrains in sensor networks such as energy, memory, computational power and challenges in sensor networks can be classified by the following criteria like cost, Mobility, Security, Routing Data aggregation. The serious issue is that the nodes may get compromised and perform various attacks. Providing Security is the biggest task in sensor network, Security solutions should be effective by providing best security and consuming less resources like energy, memory and computational power. Once the node gets compromised it performs various attacks as follows:

- Sniffing attack: Overhear Valuable data from by other nodes.[4]
- Bad Mouthing attack: Propagate negative information about Good nodes.[4]
- Good Mouthing attack: Propagate positive information about Bad nodes. [4]
- Black Hole attack: Attract the traffic to be routed as Shortest Route and Drop the packets
- Sybil Attack: Clone Several Nodes and Replica the information [4]
- Dos Attack: Prevent any part of WSN from Functioning.
- Sink Hole Attack: Attract nearby Traffic through Comprised node
- White washing attack: Using white washing attack the nodes which have their trust value less than the threshold value will try to re-enter into the system.

5. Conclusion and Future Scope

There are multiple trust and reputation techniques available to detect the selfish and malicious nodes. The basic methodologies for trust techniques and various research work under each category been addressed. Sensor applications has wide range of applications and each applications been addressed and security can be addressed and implemented in each application. We suggest for future work to provide an efficient algorithm with less consumption of energy, power and memory techniques are addressed and no compromise on the security strength is made. Self learning algorithms based on scoring system framework may be implemented further for improving the reliability of the systems, which would have advantages in terms of learning new data patterns if there is a change and thus able to identify the change fast as time changes even if the probability of factors influencing the trust factor changes due to change in scenario.

References

[1] Kazem sohraby, Daniel Minoli, Taieb znati,Wireless Sensor Networks Technology ,protocol and applications, Second edition 1991.
[2] R. Naseer, I.K. Maarouf , and M. Ashraf, “Routing Security in Wireless Sensor Networks”, Book Chapter published in Handbook of Research on Wireless Security, Publisher: Idea Group Reference, USA, 2008.
[3] Edwin prem kumar, Baskaran Kaliapermal, Elijah blessing Rajsingh “Research issues in Wireless sensor network Applications: A Survey”- International Journal of information and electronics engineering, Vol 2 No 5 September 2012.
[4] Yanli Yu,Keigiu Li, Ping Li “Trust Mechanism in wireless sensor networks: Attacks analysis and countermeasures”, Journal of networks and computer applications press 2011.
[5] Jarmillo, J Srikant R. “Darwin: Distributed and adaptive reputation mechanism for wireless adhoc networks” MOBICOM ’07 2007 p 87-98.
[6] Javier Lopez, Rodrigo Roman, Isaac Agudo, Carmen Fernandez-Gago “Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures” International Journal of information and electronics.
[7] Sun yl, Han z, YU w, Liu KJP “A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks, “IEEE INFOCOM ’06 2006 p-1-13”.
[8] Mohammad Mormani , Subash Challa ”Bayesian fusion algorithm for interfering Trust in wsn ,”Jouranl of networks” vol 5 No 7 2010.
[9] Ganeriwal, S.; Balzano, L.K.; Srivastava, M.B, “Reputation-Based Framework for High Integrity Sensor Networks”, ACM Trans. Sens. Netw. 2008, 4, 1-37.
[10] Renjian Feng, Xiaofeng Xu, Xiang Zhou and Jiangwen Wan, ”A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory”, School of Instrument Science and Opto-electronics Engineering, Beijing University of Aeronautics and Astronautics (Beihang University), Beijing 100191, China, 2011.
[11] Qi J-J Li- Z-Z Wel L.”A trust model based on Bayesian approach” Advances in Web Intelligence (AWIC), 2005 p-374-379.
[12] Afrand ,”A game theory based approach for security in wsn”, IEEE International conference on Performance ,Computing and communication 2005 p 259-263.
[13] Junhai Luo “A trust model based on fuzzy recommendations for MANET,” Computer Networks vol 53 2009 p 2396-2407.