A Survey on Detecting Selfish Nodes in Wireless Sensor Networks Using Different Trust Methodologies

Christhu Raj M R, Edwin Prem Kumar G, Kartheek Kusampudi

Abstract: - A Wireless Sensor Networks (Wsn) Is A Network Used For Computing, Sensing. There Are Various Resource Constrains In Wsn Like Energy, Computational Power, Memory, Design Challenges. The Problem In The Sensor Nodes That Nodes May Get Compromised. The Trust Management Schemes Consist Of Effective Tools To Identify Unexpected Behavior Of Sensor Nodes In The Network. Trust Has Been Effective And Provides Secure Mechanism For Managing Each Sensor Node In Network. In This Paper We Investigated Some Trust Techniques And Present The Effective Methodologies To Calculate The Trust Of A Sensor Node To Eliminate The Selfish Or Compromised Nodes In The Network.

Keywords: *Entropy, Reputation, Bayesian, Fuzzy model, Trust*

I. 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 [1] 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[6].Microcontroller are constrained devices in terms of memory and computational power. Transceivers functions towards a common goal of forwarding or routing and finally battery which determines the lifetime of each individual node. Base stations sometimes called as “Heart of Sensor Networks”. Base stations enable to collect the processed or unprocessed information from the nodes and store it for later use. Sometimes it issues some control orders to modify the behavior of sensor node. The sensor nodes are designed to perform the functions like Monitoring, Alerting, Information on Demand,Actuating.Based on applications sensor networks can be classified into C1WSN (Category 1 Wireless sensor networks) and C2WSN (Category 2 Wireless Sensor Networks). In C1WSN it is mesh-based systems with multi-hop radio connectivity and in C2WSN it is point to point or multipoint-to-point systems with one or single hop radio connectivity[1][3]. The various applications includes health monitoring, home control, Building Industrial automation, Medical applications, Highway monitoring, Military application, Habitat monitoring, Wildlife and Instrumentation.

A. Research Issues and Resource Constrains:-

The various research issues includes [2] Biological applications- Biological Task mapping, Biomedical signal monitoring. In Commercial applications includes – Smart parking, Vehicular Telematics, Security of Intra-car, Event Detection, Structural Health Monitoring. In Environmental application the research issues are as follows, Green house monitoring, Habitat Surveillance. The various resource 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 series issues 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 nodes gets compromised it performs various attacks as follows:

1. Sniffing attack: Overhear Valuable data from by other nodes.[4]
2. Bad Mouthing attack: Propagate negative information about Good nodes.[4]
3. Good Mouthing attack: Propagate positive information about Bad nodes. [4]
4. Black Hole attack: Attract the traffic to be routed as Shortest Route and Drop the packets
5. Sybil Attack: Clone Several Nodes and Replica the information [4]
6. Dos Attack: Prevent any part of WSN from Functioning.
7. Sink Hole Attack: Attract nearby Traffic through Comprised node
8. 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.
9. Intelligent Behavior attack: According to the intelligent behavior attack the nodes may provide good or bad services according to the threshold of trust rating.

To provide secure network the need of trust management in encountered. Trust is a security mechanism that can be used to detect the unexpected behavior of nodes in the network.

Manuscript published on 30 February 2013.
* Correspondence Author (s)

Christhu raj M.R, PG Scholar , Department of Information Technology, Karunya University, Karunya Nagar, Coimbatore, Tamil Nadu, India.
G .Edwin Prem Kumar, Assistant Professor, Karunya University, Karunya Nagar, Coimbatore, India.
K. Kartheek, , PG Scholar , Department of Information Technology, Karunya University, Karunya Nagar, Coimbatore, Tamil Nadu ,India.

There is various trust techniques used to detect the nodes and eliminate the selfish nodes. Section I detailed overview of Wireless sensor networks and its applications, challenges are presented. Section II deals with need and importance of trust management in sensor networks and In Section III, the various trust evolution models are presented and in Section IV deals with various comparison of trust techniques are presented.

II. IMPORTANCE OF TRUST IN SENSOR NODE

The Present-day Sensors may be considered as a human being like they are produced in a controlled environment and has single goal [6]. These nodes can perform simultaneously various operations and forward the sensed data to base-station. Latest technology sensors mainly used to sense the data and process on the data then forward the processed data to neighbor's nodes using one hop or multihop communication. The basic architecture of the nodes depends on application and functions that are intended to perform. Since the nodes sends the data to base station the medium being air an intruder can eavesdrop the sensed data. Sometimes an intruder can capture the packet and modify the values, change the behavior of nodes which will result in complete loss of system. To overcome the problems there is a need of proper security mechanism. Trust is one of the security mechanism used to detect the behavior of nodes and builds a self-healing network. Trust development can be in the following fields authorization (Hard trust) and evaluation (Soft trust) [7].

Policy maker was the first trust management scheme proposed by Blaze et al (1996) [8].It was based on cryptographic techniques where a trusted third party signs a certificate message to certify the identity associated with a public key.

III. TRUST METHODOLOGIES

A. Bayesian trust model

Bayesian Trust methodology been used in research work [9] [10] [11] to detect the selfish nodes. The 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].

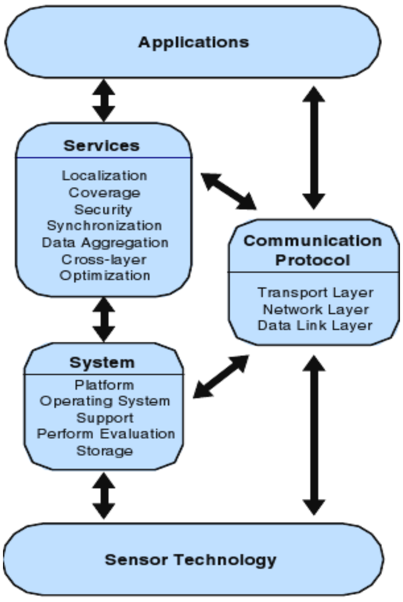

Figure 1: Classification of Various issues

B. Game theory trust model

Game theory model tries to capture the behavior of nodes mathematically in situations where the decisions depend upon the behavior of the other nodes. Trust mechanism [12][13] based on game theory have been implemented to detect the selfish nodes

C. Entropy trust model

The concept of thermodynamics is used where entropy deals with how much uncertainty is there in a signal or event.[9] proposed a method for trust evaluation in adhoc networks which uses Bayesian model and entropy model

D .Fuzzy trust model

IF-THEN rules is 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.

These above listed models are few methods used to calculate the trust of individual nodes and detect whether a node is selfish or compromised nodes.

IV. EVOLUTION OF TRUST

A. Based on Reputation Systems

***Ganeriwal et al* [14]** proposed a reputation based trust system to detect the selfish nodes. In this system a framework has been developed using Bayesian formulation specifically beta reputation system, reputation representation, updates and integration. The method employs watch-dog mechanism to calculate the reputation. 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. Ultimate trust calculation depends on additive of watchdog mechanism, secondhand information and Reputation. The main disadvantage is trust evaluation is based only on node's Qos property and flat wsn architecture followed which is not scalable.

Mohammaed momani et al [15] proposed a trust mechanism to combine more than one trust component. The proposed Algorithm in the paper is simple and generic as it allows trust components to be added or deleted. The main advantage of the work highlights the fact that one trust component is not enough to calculate the trust and introduces data trust and communication trust. The trust value is addition of first hand and second hand parameter which is based on beta reputation methodology

S.Ozdemir et al [16] proposed a trust scheme where selfish nodes or compromised nodes tries to malfunction the network distort the data integrity by appending false data during aggregation and disturbing the transmission of aggregated data. To overcome this problem RDAT protocol which is based on concept of Functional reputation were it improves the reliability of data aggregation and it employs Reed-Solomon coding scheme to ensure the reliable data transmission to the base station. Ultimate trust calculation is based on Routing, sensing, aggregation (Time stamped value).

Alzaid, Hani et al [17] proposes a data aggregation for wsn that integrates aggregation functionality . It is based on beta reputation methodology to improve the network lifetime and the integrity of the aggregated data. It uses the symmetric secret keys to assign keys to sensor nodes bases on their locations. It is similar to watchdog mechanism and reputation table consists of sensing, actuating, fowardbased reputation values.

Zahra et al [18] proposed energy efficient trust based algorithm where it concentrates on aggregation and energy. The concept of functional reputation and trust is used to select nodes that best satisfy the criteria to be an aggregator on the basics of quality of the node . In order to find best path from every sensor node the link availability and residual energy of nodes are taken into account. The disadvantage of the ETA introduces some delays in the network but overall it outperforms in terms of reliability and lifetime (Energy).

E fthimia et al [21] proposed a reputation management system where a trust management model is developed with predefined roles and capabilities. This allows the information flow and flexibility in the trust establishment process. It is a hybrid model which combines certificate-based and behavior based approaches on trust establishment. It enables controlled trust evolution an controlled trust revocation. The disadvantage of related work is only node's Qos property considered and it follows a flat wsn architecture which is not scalable.

B. Based on Entropy Model

Sun yl et al [9] proposed a trust model to detect selfish nodes and malicious modes. It represents a framework to measure trust, trust propagation model and defend trust evaluation against attacks. It gives a clear understanding of trust metrics, mathematical properties of trust, dynamic properties of trust and trust models. Possible attacks against the proposed system has been identified(Sybil attack) and various remedial techniques been applied. This system improves the routing techniques and improves the throughput of network. It uses both entropy model and Bayesian model. The trust evaluation is proposed for ah-hoc networks

Dai Hongjun el al [23] this method uses a novel entropy based model and evaluation methods to find trust. To summarize the work first entropy based trust calculation model is found to get the trustworthiness between two nodes. Next to get the trust value from one node to another using direct action a probability action [0,1] is followed. Third step the trust is established between nodes using recommendations and directed graph is used to describe the trust values.

C. *Based on Game theory model*

Jaramillo et al [12] proposed a Distributed and adaptive reputation mechanism for wireless adhoc networks. It follows a technique were a retaliation situation can be avoided after anode which has been falsely perceived as a selfish nodes and the cooperation can be restored between the nodes.

Komathy k et al [13] presents a multiple nodes to build trust and an effective, dynamic and distributed framework using game theory. The model brings out two distinct modes to learn and predict the behavior of the neighbors namely deterministic and random. In the first deterministic mode it is a generic one which aids in finding out behavior of the network for standard patterns. The random mode are explored using randomized analysis based on genetic algorithm. Game theory gives a suggestion about how the participants have to behave.

Afrand et al [24] based on cooperative game theory proposed a game between a sensor node and three factors namely cooperation, reputation and quality of security. 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.

D. Based on Fuzzy model system

Azzedine Boukerche et al [19] proposed a trust system for pervasive and ubiquitous computing. 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. Through this system a formal security analysis of trust system is proposed and malicious nodes are detained from pervasive and ubiquitous computing

Fleix Gomez et al [20] based on calculating trust in VANET.TRIP aimed to quickly and accurately distinguish malicious or selfish nodes spreading false or bogus messages throughout the network. The level of fulfillment of each of the surveyed models with regard to each design requirement suggestion, comparing them with this approach.

Junhai Luo et al [22] proposed a trust scheme where sensor has constrained resources of sensor like energy, bandwidth, and memory.RFSTrust based on fuzzy recommendation. This includes five types of fuzzy trust recommendation relationships based on the fuzzy relation theory and a mathematical description for MANETs. Fuzzy logic provides a natural framework to deal with uncertainty and the tolerance of imprecise data inputs for the subjective tasks of trust evaluation, packet forwarding review and credibility adjustment.

V. TRUST BASED ON QOS SOCIAL NETWORK

There are many trust work based on Qos and social networks. [25] Proposed a trust management scheme based on location verification where the security of geographic routing is considered. In this method geographic routing neighbors exchange about location information. This address the attacks falsifying location information and proposes a trust-based multipath routing. Riaz et al [26] proposes a group based trust management scheme for clustered wsn where a new lightweight protocol been developed. It reduces the cost of overhead and well suits for large scale networks. The evaluation was based on direct observations. The unique feature of GTMS is that trust works on two groups Intra and inters group topology and GTMS provides mechanism to detect and prevent the attacks. The drawback of GTMS protocol is trust value is based on past interactions and trust formation issue to maximize application is not addressed. It is not scalable too.

VI. CONCLUSION AND FUTURE SCOPE

They are multiple trust and reputation techniques available to detect the selfish and malicious nodes.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

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 an security can be addressed and implemented in each application. Providing efficient algorithm with less consumption of energy, power and memory techniques are addressed.

REFERENCES

[1] Kazem sohraby , Daniel Minoli , Taieb znati,*Wireless Sensor Networks Technology ,protocol and applications,* Second edition 1991

[2]. 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

[3]. Kazem sohraby *Applications of Sensor networks*. First edition 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]. Javier Lopez, Rodrigo Roman, Isaac Agudo, Carmen Fernandez-Gago “Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures”, *Journal of Network and Computer Applications*

[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]. I.F.Akyildiz,.Su Y.Sankara E. Cayirci “Wireless sensor networks:a survey

[8]. Blaze M, Feigenbaum J, Lacy J. “Decentralized trust management”. *In: Proceeding of the 1996 IEEE symposium on security and privacy,* Washington, 1996. p. 164–73.

[9]. 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”

[10]. Nielsen N , Krukow K , Sassone V , Model for event-bases trust” *Electronic Notes on Theortical Computer Science (ENTCS) 2007 ,* vol 172,2007 p 499-521

[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]. Jarmillo, J Srikant R. “Darwin: Distributed and adaptive reputation mechanism for wireless adhoc networks” *MOBICOM ’07 2007* p 87-98

[13]. Komathy K. Narayanasamy P. “Trust-AODV routing against selfishness”,*Journal of Network and Computer applications* vol 31 , Issue 4 ,2008 p 446-471

[14]. S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, “Reputation-based framework for high integrity sensor networks,” *ACM Trans. Sensor Networks.*, vol. 4, no. 3, pp. 1–37, May 2008.

[15]. Mohammad Mormani , Subash Challa ”Bayesian fusion algorithm for interfering Trust in wsn ,”*Jouranl of networks*” vol 5 No 7 2010

[16]. Suat Ozedemir , “Functional reputation based reliable data aggregation and transmission for Wireless Sensor Networks” *Computer communications* vol 31 2008 p 3941-3953

[17] Hani Alzaid , Ernest Foo , Juan Nieto “RSDA Reputation-based secure data aggregation in Wireless sensor networks”, *International conference on Parallel and distributed applications and technologies , 2008*

[18] Zahra Taghikkaki “Energy efficient Trust based Aggregation in WSN ” *INFOCOM WKSHPS ‘2011* 2011 p 584-589

[19] Boukerche A.Ren “A trust based security system for ubiquitous and pervasive computing”, *Computer Communications* vol 31 Issue 18,’08

[20] Felix Gomez “TRIP, a trust and reputation infrastructure-based proposal for VANET ” *Journal of Network and Computer Applications*

[21] E. Aivaloglou and S. Gritzalis, “Hybrid trust and reputation management for sensor networks,” *Wireless Networks*, vol. 16, no. 5, pp. 1493–1510, July 2010.

[22]. Junhai Luo “A trust model based on fuzzy recommendations for MANET ”, *Computer Networks* vol 53 2009 p 2396-2407

[23]. Dai Hongjun “An entropy based trust modeling and evaluation for Wireless sensor networks” *International conference on Embedded Software systems* ,ICESS 2008

[24]. Afrand ,”A game theory based approach for security in wsn”, *IEEE International conference on Performance ,Computing and communication 2005 p 259-263*

[25] K. Liu, N. Abu-ghazaleh, and K. D. Kang, “Location verification and trust management for resilient geographic routing,” *J. Parallel Distrib.Computing*, vol. 67, no. 2, pp. 215–228, Feb.07.

[26] R. A. Shaikh, *et al.*, “Group-based trust management scheme for clustered wireless sensor networks,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 11, pp. 1698–1712, Nov. 2009.