RESEARCH PAPER | Engineering | Volume : 4 | Issue : 1 | Jan 2014 | ISSN - 2249-555X

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

KEYWORDS: Entropy, Reputation, Bayesian, Fuzzy model, Trust

Dr.ArunKorath
Director of P.G.Studies, Vedavyasa Institute Of Technology, KaradParamba, Malappuram, Kerala

Vineeth K.V
S8 Student B.Tech CSE, Vedavyasa Institute Of Technology, KaradParamba, Malappuram, Kerala

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.*

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 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 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:

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.

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. 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 basestation. 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 com-

Volume : 4 | Issue : 1 | Jan 2014 | ISSN - 2249-555X

munication. 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.

TRUST METHODOLOGIES

Bayesian trust model

Bayesian Trust methodology been used in research work [9] [10] [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].

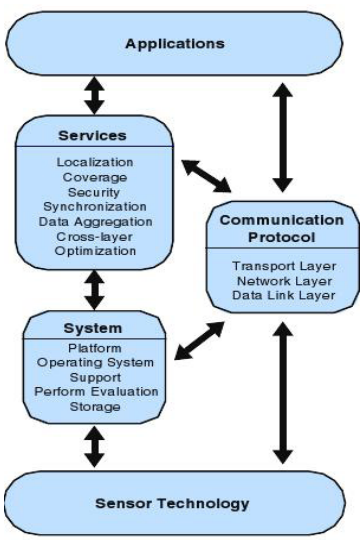

Figure 1: Classification of Various issues

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.

V. TRUST BASED ON QOS SOCIAL NETWORK

There are many trust work based on Qos and social networks. 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 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. 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.

REFERENCE

[1]Kazem sohraby , Daniel Minoli , Taieb | znati, Wireless Sensor Networks Technology ,protocol and applications,Second edition 1991 | [2].Edwin prem kumar, Baskaran aliapermal, 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