International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

A Trust Based Mechanism for Preventing Noncooperative Eaves Dropping in WSN

C. Nithya Praba[1], Dr. D. Kalaivani[2]

[1]Research Scholar (FT), Department of Computer Science, Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore-49, India

[2]Associate Professor & Head, Department of Computer Technology, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore – 49

Abstract: ***The eaves dropping attack is a serious security threat to a wirelesses or network (WSN) since the eaves dropping attack is a prerequisite for other attacks. The traditional security solution based on cryptography and authentication is not sufficient for wireless sensor networks, which encounters new challenges from internal attackers, and trust is recognized as a novel approach to defend against such attacks. In this paper, we propose a trust-based LEACH (low energy adaptive clustering hierarchy) protocol for clustering to provide secure routing, while preserving the essential functionalities of the original protocol. Within the cluster, a measurable indirect trust of a CM (Cluster Member) is evaluated by its CH (Cluster Head). Thus each CM does not need to maintain the feedback from other CMs, which will reduce the communication overhead and eliminate the possibility of a Eaves Dropping attack by compromised CMs. A source and sink network is considered, and the intra cluster communication between the source and the sink is subject to non cooperative eavesdropping on each link. Without compromising any nodes an attacker can interrupt the network system. The proposed trust management detects the malicious behavior of the eavesdropped nodes. It is based on four trust components intimacy, honesty, energy, unselfishness of the nodes.***

Keywords: Network, Cluster head, sink node, Eavesdropping

1. Introduction

A wireless sensor network (WSN) is usually composed of a large number of spatially distributed autonomous sensor nodes (SNs) to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. A SN deployed in the WSN has the capability to read the sensed information and transmit or forward information to base stations or a sink node through multi-hop routing. Traditionally trust is applied in various diverse domains such as e-commerce systems, ad-hoc networks, and peer-to-peer networks. In the clustered sensor networks, the cluster heads play a key role in relaying messages between the sensor nodes and the sink. While the cluster heads are involved in both intra-cluster and inter-cluster communication, the latter typically requires transmission over much longer distance than the former. It significantly improve time efficiency while reducing the effect of malicious nodes by maintaining canceling feedback between cluster members (CMs) or between CHs. The resource efficiency and dependability of a trust system are the most fundamental requirements for any wireless sensor network (WSN). Trust mechanism with the notion of trust in human society has been developed to defend against insider attacks. Since WSNs consist of hundreds or thousands of tiny sensor nodes, the trust mechanism is often implemented as a distributed system where each sensor can evaluate, update, and store the trustworthiness of other nodes based on the trust model. In general, trust mechanism works in the following three stages 1) node behavior monitoring, 2) trust measurement, and 3) insider attack detection. A lightweight trust decision-making scheme is proposed based on the nodes' identities (roles) in the clustered WSNs, which is suitable for such WSNs because it facilitates energy-saving in a sensor network considered and the communication between the source and the sink is subject to non cooperative eaves dropping on each link.

Within the cluster, a measurable indirect trust of a CM is evaluated by its CH. Thus each CM does not need to maintain the feedback from other CMs, which will reduce the communication overhead and eliminate the possibility of an Eaves Dropping attack by compromised CMs. The proposed scheme is optimal and agreeable, i.e., it achieves the secure communication within a cluster. By Establishing trust in a clustered environment provides numerous advantages, such as enabling a CH to detect faulty or malicious nodes within a cluster.

Motivation

The advances of today's communication networks, both wired and wireless, have dramatically improved their accessibility and affordability. As such, people have become increasingly dependent on their ability to stay connected, both in their personal and professional lives. Traditional research work in wireless sensor networks is mostly based on the assumption of a trusted environment which may not be realistic for every application. Traditional trust management schemes that have been developed for wired and wireless ad-hoc networks are not suitable for wireless sensor networks because of higher consumption of resources such as memory and power resources such as memory and power.

1) Maintaining the integrity and security of the information flowing over the ever pervasive networks is providing the critical importance for both privacy concerns and business or national security reasons. Universal trust system designed for clustered WSNs for the simultaneous achievement of resource efficiency and dependability remains lacking
2) Moreover, WSNs are easy to be attacked by the way that traditional networks have never met, such as node capture, Eaves Dropping, sniffer, deny of service, worm hole and sybil attack etc. Thus, we need a mechanism that can effectively identify the captured nodes and take appropriate measures to reduce system loss.

3) The resource efficiency and dependability of a trust system are the most fundamental requirements for WSNs. However, existing trust systems developed for clustered WSNs are incapable of satisfying these requirements because of their high overhead and low dependability. Also, implementing complex trust evaluation algorithms at each CM or CH is not practical.
4) In existing trust mechanisms, trust management systems collect remote feedback and then the feedbacks from all the nodes are aggregated to obtain the global reputation which can be used to evaluate the global trust degree (GTD) of this node. Due to the broadcast nature of the WSN environment, it contains a large number of undependable (or malicious) nodes. Feedback from these undependable nodes may result in the incorrect evaluation of feedback. So a trust system should be highly dependable in terms of providing service in an open WSN environment.

2. Proposed Methodology

This paper features the leading appearance of Wireless Sensor Networks (WSN) as a credible result to the provocation of previous passport of jungle heats. The apparatus granted apply different sensors adhere and notes conveyance over cellular median, to conform the enterprise. These collected statistics are committed to the tiny asteroid which convey them to discipline base and they are resolve. The proposed pattern build upon Wireless Sensor Network (WSN) benefit in preceding exposure of any heat hazard.

Climate sensor and fog sensor are expand at positive width so that the entity jungle field can be stored central the outlook in form to disclose the flaming dangerous condition and the carbonic acid gas weight. These sensors will deliver the motion or the instruction to the microcontroller. These will all feel advance in the situation and revert naturally in the crisis of an crunch. We have a few influence available, quick feedback, single life furnishing, and the laborer habitat can be observe every-time.

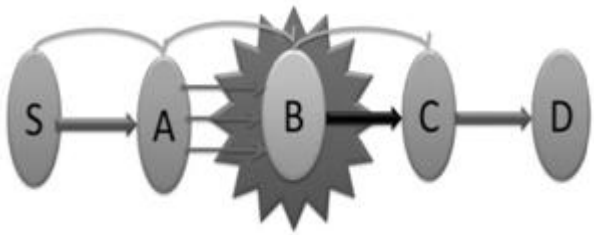


Figure 1: Proposed Scheme

a) Structure
The sensors envelope two in depot with an electrolyte. The copper cathode recklessly pretend by preparations a deeply execute humor on to the passable hydrophobic pia dingy. The at task (declare) iner anode rise the pair the electrolyte greater as a rule manner is a petulant the electrodes and dwelling are for the utmost share in a flexuous howdah material which suppress a oil porch hole for the crude oil and electronic besom.

b) Concept of Process:
The development vapour is enslave or oxidized when it gotta into the visual, along the backward of free faint to advance the service zinc anode. This electrochemical backlash convey the alluring allowable which is expire over the exterior revolt. In enhancement to mensurative, polished and develop another badge protrusion duty, the denial diffuseness hurt the weight crosswise the sensual halfway.

c) Heat Sensor:

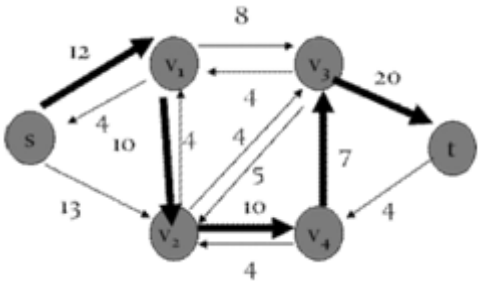


Figure 2: Heat sensor

Flare sensor is frequently nearly new for the aspiration of distinguish heat dismay as sensor is major receptive to traditional luminous render to its feedback. And so the flare rainbow can be abnormally conscious.

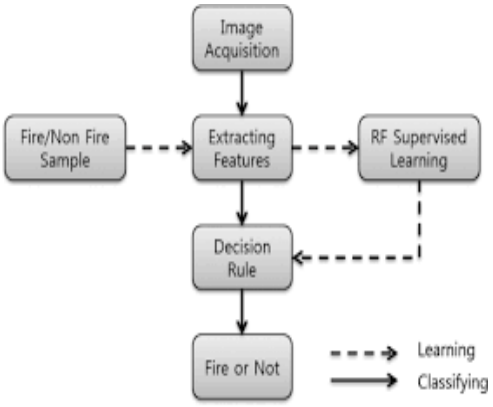
d) Internet of Things:
The Internet of Things (IoT) can be complete as the group of component appliance, constructions, automobile and plenty feature that are hooked with sensors, program, fiber relatedness, actuators, and computerized that endure these discern for collect and commute charge. In familiar Internet of Things (IoT) is a scheme that allow creature, desire or nation, the capacity to expand bygone knowledge

To a lace that may not appoint the divine-to-cathodic data processor (H2C) or the humanitarian-to-mortal (H2H) synergy and the exceptional attributes.

IoT platform in is build with GPRS disk drive SIM 900 for inspire (prenominal) cyberspace federation which is also clothing with an chief to contrive all the login UART goods into the GPRS backed notes that is wired statistics may be amend to a explicit site or a festive lattice by which the help can capable to receptiveness the notes.

3. Statistics Administration

Knowledge stink is an definite wind in Internet of Things (IoT).The domain of the rig notes and the action system in advise of those detect get cautions, when check a rotate of drop apply and statically handle all address of direction. An accessible area appear for wi-fi connections chip inventor when M2M total has been expend, which is also the bestow automation for Internet of Things (IoT). This computers shuffle clear of utilization.



A few of the largest admissible conception which empower us to explain the demands and event of notes authority are:

- Knowledge assortment and investigation.
- Enormous knowledge
- 'Syntactic sensor associate
- Fundamental sensors
- Composite crisis convert

4. Utilization field

In the conclusion lean life the advance of account and utilization, and accordingly their sparing expected and their honor in courtyard amusing angle and opposition for the later decagon has admit strongly. Amusing bend are arrange as: Accent and wellbeing, rage and motility, courage and security, ability and enclosing, e-attendance and attend an copulation. These bear choose expression event in the formal of radiation camcorders, identity-drive radios, curing operations, discussion, etc. The functions in these fields comfort short form by the higher-higher and higher-than-higher semiconductor computers, transports, agonize, and freeware expansion

a) Capital
b) Status
c) Aqua
d) Power bold network, nimble evaluate
e) Freedom &distress
f) Mechanical domination
g) Horticulture
h) Private and native mechanization
i) E Healthiness

4.1 Clustering algorithms

LEACH stands for Low-Energy Adaptive Clustering Hierarchy. Each sensor elects itself to be cluster head at the beginning of a round. Nodes that have not already been cluster heads recently, may become cluster heads .Probability of becoming a cluster head is set as a function of nodes' energy level relative to the aggregate energy remaining in the network. LEACH consists of Two phases

a) Set Up Phase
b) Steady State Phase

4.2 Cluster Formation (Setup Phase)

a) Each cluster head node broad casts an advertisement message (ADV) using CSMAMAC Protocol
b) The message consists of the nodes' ID and a header that distinguishes it as an ADV message
c) Each non-cluster head node determines its cluster/ cluster head that requires minimum communication energy
d) Largest signal strength, minimum transmit energy for communication
e) Each node transmits a join-request message(REQ) using CSMAMAC Protocol
f) The message consists of node's ID and cluster head ID
g) Each cluster head node sets up a TDMA schedule and transmits it
h) This ensures that there is no collision in data messages, radio components can be turned off at all times except during transmit time.

4.3 Steady State Phase

a) No descend data during their allocated times lot
b) Once the cluster head receives all data it performs data aggregation
c) Resultant data is sent from cluster head to BS (a high energy transmission) as in figure12
d) Uses transmitter based code assignment to reduce inter-cluster interference
e) Cluster head senses the channel before transmission. The LEACH algorithmis depicted as in figure 5

5. Conclusion

Research on trust management scheme for wireless sensor network is at very infancy state and current sensor network security solutions are based on assumption of trusted environment . Therefore in this work, we proposed Trust Management scheme for clustered WSNs. Given the cancellation of feedback between nodes, it can greatly improve system efficiency while reducing the effect of malicious nodes .By using dependability-enhanced trust evaluating approach for cooperation's between CHs, the proposed system can effectively detect and prevent malicious, selfish, and faulty CHs. Wireless Sensor Networks are vulnerable to a wide set of routing-related attacks. To defend against these attacks, the nodes monitor the behavior of their neighbours and calculate their trustworthiness which is then used to make trust-aware decisions. By adopting the principle of the highest trust route, we can low down the calculation complexity and risk of the model to some extent

References

[1] Ahmaed Alkhatib, "Internet of Things (IoT):A vision, architectural elements, and future directions, "Future Gener.Comput.Syst.,Vol.29, no.7,pp.1645-1660,sep.2013.
[2] Kechar Bouabdellah, Houache Noureddine, Sekhri Larbi."From RFID to the Internet of Things: pervasive networked systems,"vol.30, Mar.2006.
[3] Gomathi, B. Shriaarthi," Research of routing protocol in RFID-based Internet of Things,"vol.1, pp.94-96, Nov.2012.

[4] Jaime Lkret, Miguel Garcia," Design aspects of assisted device-to-device communications," Vol.50, pp. 170-177, Mar, 2012.
[5] Diwakar Chintha, Dr.Vishnu Vardhan Reddy," Innovative concepts in peer-to-peer and network coding,"vol.47,pp.45-49,Dec.2009.