Role Based and Energy Efficient Trust System for Clustered Wsn

S. Jeyantha Jafna Juliet [1], M. Varghese[2]
[1(]*Infant Jesus College of Engineering & Technology)*
[2(]*Assistant Professor Infant Jesus College of Engineering &Technology)*

Abstract: *Security and trust are two interdependent concepts and are often used interchangeably when defining a secure wireless sensor network (WSN) system .However, security is different from trust in that, it assumes no node is trustworthy and requires ongoing authentication using sophisticated protocols leading to high communication and computation overheads. This makes the traditional cryptographic security tools hard, if not impossible, to be used in wireless sensor networks that are severely resource constrained. Trust on the other hand is the exact opposite of security in that any node can interact with any other and requires no authentication and mapping of hidden keys to carry on with their business and hence carries zero overhead. Trust management scheme calculates the trustworthiness of the node. Several trust systems have been proposed for the WSN.But they suffer from various limitation such as high cost and overhead. So light weight trust system is necessary because of the node's resource constrained nature. This proposed system provides light weight trust decision making and it improves the dependability of the system by cancelling the feedback between clustered members. It uses self adaptive weighting scheme for trust aggregation. Thus, it needs less memory and communication overhead.*

I. Introduction

Wireless Sensor Network

Wireless sensor networks (WSNs) are becoming increasingly attractive for numerous application areas, such as military reconnaissance, disaster management, security surveillance, habitat monitoring, medical and health, industrial automation. Thus, WSNs have managed to establish the connection between the physical world, the computing world and human society. In general, a WSN consists of a large number of tiny sensor nodes distributed over a large area with one or more powerful sinks or base stations (BSs) collecting information from these sensor nodes. All sensor nodes have limited power supply and have the capabilities of sensing, data processing and wireless communication. All these nodes process and forward their signals through a wireless channel to the base station that, based on that information, provides a number of services to an external system as shown in the figure 1.1

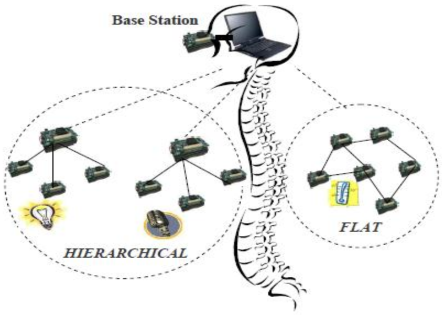


Fig. 1.1 Overview of the Architecture of WSN

II. Security In Wireless Sensor Networks

Since sensor networks is a young technology there are many interesting research problems, like development of models and tools for the design of better WSN architectures, elaboration of standard protocols adapted to work robustly on certain scenarios, etc. However, one of the most important issues that remain mostly open is security. Sensor nodes are highly constrained in terms of computational capabilities, memory, and communication bandwidth and battery power. Additionally, it is easy to physically access the nodes because they must be located near the physical source of the events, and they usually are not tamper-resistant due to cost constraints. Furthermore, any device can access the information exchange because the communication channel is public. As a result, any malicious adversary can manipulate the sensor nodes, the environment, or the communication channel for its own benefit. For these reasons,it is necessary to provide the sensor network with basic security mechanisms and protocols that can guarantee a minimal protection to the services and the information flow. This means to provide protection on the hardware layer, the communication stack, and the core protocols". In other words, (i) it is necessary to protect the hardware of the nodes against attacks, (ii) the communication channels must meet security goals (like confidentiality, integrity and authentication), and (iii) the core protocols of the network must be robust against any possible interferences.

III. Trust Management For Wsn

Trust is a very important factor in the decision-making processes of any network where uncertainty is a factor. Management system: if an element of the network knows in advance the actual behaviour of their partners (e.g. collaborative, malicious, and faulty), it can make a flawless decision. All the elements of the network work towards the same goal, and they have neither reason nor the will to behave egoistically. On the other hand, a sensor node does not have information regarding others that will allow it to know in advance how a transacting partner is going to behave. Therefore, there is some information asymmetry that the node must deal with. When a sensor node chooses a partner to collaborate with, such partner is supposed to be honest and fully collaborative. Sensor networks can suffer the attack of malicious nodes or the existence of faulty nodes. As a result, uncertainty in sensor networks is a problem that must be dealt with a Wireless Sensor Network must be able to configure itself during its lifetime in presence of extraordinary events.

Trust Management Architectures for WSN

For sensor networks, it is necessary to have a lightweight distributed architecture that tries to assure coverage of the whole network. This architecture must be behaviour-based in order to react to the events that may occur during the lifetime of the network. These requisites are given by the decentralized nature of WSN and its specific characteristics and constraints.

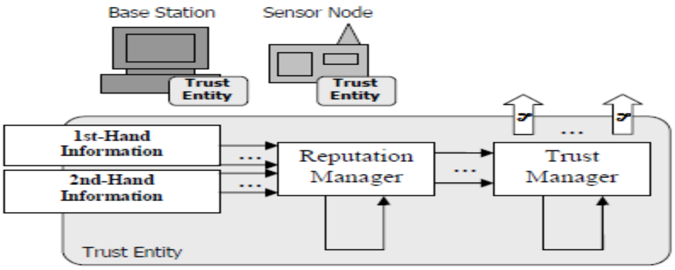


Fig 1.2. Structure of a Trust Entity for Sensor Networks

An important element of any trust management system is the trust entity. This entity is in charge of obtaining, calculating and maintaining reputation and trust values. For sensor networks, it is possible to define the structure of a generic trust entity, as shown in Figure 1.2.

Trust and Reputation Monitoring System

A system that makes the use of trust and reputation information to calculate the trustworthiness of a node is called a TRM. Such a system must be able to judge a node's misbehavior and effectively distinguish between normal operating and malicious node. In TRMs, the positive and negative effects of a node's action are observed. The observations are aggregated in a specific trust table maintained by the node. Statistical analysis is performed on the trust table data to generate the node reputation.

IV. Analysis

System Analysis Existing System

The resource efficiency and dependability of a trust system should undoubtedly be the most fundamental requirements for any WSN (including clustered WSNs). However, existing trust systems developed for clustered WSNs are incapable of satisfying these requirements because of their high overhead and low dependability. A universal trust system designed for clustered WSNs for the simultaneous achievement of resource efficiency and dependability remains lacking. First, limited work has focused on the resource efficiency of clustered WSNs. A trust system should be lightweight to serve a large number of resource-constrained nodes in terms of accuracy, convergence speed, and additional overhead Furthermore, limited work has focused on the dependability of the trust system itself. In existing trust mechanisms for WSNs, trust management systems collect remote feedback and then aggregates such feedback to yield the global reputation for the node that can be used to evaluate the global trust degree (GTD) of this node. However, an open or hostile WSN environment contains a large number of undependable (or malicious) nodes. Feedback from these undependable nodes may yield incorrect evaluation. The dependability of a trust system is undoubtedly an important requirement for any WSN environment. That is, a trust system should be highly dependable in terms of providing service in an open or hostile WSN environment. However, most previous studies lack feasible alternatives to solve the problem of malicious feedback, which significantly affects system dependability and feedback availability. Recent studies for clustered WSNs TCHEM , HTMP the authors adopt simple weighted average approaches to aggregate feedback trust information without considering the problem of malicious feedback. This may result in misjudgment of the trust decision-making process.

Proposed System

This proposed System has the following features

1*)* A lightweight trust evaluating scheme for cooperations between CMs or between CHs. Within the cluster, the 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 a bad-mouthing attack by compromised CMs. The feedback of a CH is applied a similar manner to obtain the same benefits.

2) A dependability-enhanced trust evaluating approach for cooperations between CHs. Considering that CHs take on large amounts of data forwarding and communication tasks, a dependability-enhanced trust evaluating approach is defined for cooperations between CHs. This approach can effectively reduce networking consumption while preventing malicious, selfish, and faulty CHs.

3) A self-adaptive weighting method for CH's trust aggregation. This approach overcomes the limitations of traditional weighting methods for trust factors, in which weights are assigned subjectively.

V. Modules

Project Overview

The resource efficiency and dependability of a trust system are the most fundamental requirements for any Wireless sensor network (WSN). Existing trust management systems developed for clustered WSN are incapable of satisfying these requirements. Most of the works failed to consider the resource constraints of nodes and collect remote feedback from the undependable nodes also. The dependability of a trust system is also important. The aim of this project to develop a light weight and dependable trust system for clustered WSN as well as a mechanism that reduces the likelihood of compromised or malicious node being selected as a collaborative node. Nodes are organized into clusters. A node in the Clustered WSN can communicate with their CH directly. A CH can forward aggregated data to the BS through other CH's. The features of this project are 1) A light weight evaluation trust evaluating approach for cooperation between cluster members or cluster heads. Within the cluster, the indirect trust of a CM is evaluated by its CH. Thus each CM does not need to maintain the feedback from other CM's which will reduce the communication overhead. 2) A dependability enhanced trust evaluating approach for cooperation between CH's.3) Self adaptive weighting method for CH's trust aggregation instead of traditional weighting methods for trust factors.

Network Formation and Clustering Process

In this module, nodes are created and deployed in the Wireless sensor network. The nodes are labeled as CH, CM or BS. Then the cluster head is elected and the cluster is formed. The cluster head is not selected randomly. The cluster construction is based on the node's residual energy and communication cost. Initially, all the nodes have uniform energy. After doing some operation the energy will be reduced. The node with relatively high average residual energy compared to other CM's will be elected as CH. When a node is elected CH successfully, it broadcasts an advertisement message to the other nodes. According to the received signal strength of the advertisement, other nodes decide to which cluster it will join and send a membership message to its CH.

Intra Cluster Trust Calculation

In this module, the CM-CM direct trust and CM-CH feedback is calculated. The total number of successful and unsuccessful interactions is calculated for every pair of nodes in the cluster for some period of time. Then the CM-CM direct trust is evaluated based on the following equation

$$Tx,y(\Delta\mathrm{t}) = \frac{10 \times Sx,y(\Delta t)}{Sx,y(\Delta t) + Ux,y(\Delta t)} \times \frac{1}{\sqrt{Ux},y(\Delta t)}$$

Where Δt is a window of time. sx;y(Δt) is the total number of successful interactions of node x with y during time Δt,ux;y(Δt)≠ 0 is the total number of unsuccessful interactions of node x with y during time Δt.

For CH-CM indirect trust calculation, direct trust values from each cluster members is sent to the CH periodically.CH maintains the trust values in a matrix. Then Beta probability density function based on the positive and negative feedback is used to calculate the indirect trust.

$$Rch,y(\Delta t) = 10 \times E(\rho(p\backslash r,v)$$

$$E(\rho(p\backslash r,v) = \frac{r+1}{r+v+2}$$

Inter Cluster Trust Calculation

In this module, the direct trust between CH-CH direct trust and BS-CH feedback is calculated. The direct trust between one CH to another CH is calculated using the following formula

$$Ci,j(\Delta t) = \frac{10 \times Si,j(\Delta t)}{Si,j(\Delta t) + Ui,j(\Delta t)} \times \frac{1}{\sqrt{Ui,j(\Delta t)}}$$

Si;j(Δ*t*) is the total number of successful interactions of CH *i* with CH *j* during time window Δ*t*, and *Ui;j*(Δ*t*) is the total number of unsuccessful interactions of CH *i* with CH *j*.To calculate the BS-CH feedback trust, the direct trust value of each CH is sent to the BS periodically. These direct trust values are maintained in matrix. Then the Beta probability density function

$$Fbs,j(\Delta t) = \frac{10 \times E(\rho(p\backslash g,l) + ck,j(\Delta t)}{2}$$

is used to calculate the feedback trust. Where *g* is the amount of positive feedback ($Ck;j \geq 5$) towards a CH *j*, and *l* is the amount of negative feedback ($Ck;j < 5$).

$$E(\rho(p\backslash g,l)) = \frac{g+l}{g+l+2}$$

$$ck,j(\Delta t) = \frac{\sum Ck,j(\Delta t)}{g+l}$$

Is the average value of aggregated feedback from ($g + l$) CHs in the network.

Trust Aggregation at CH level

In this module, the global trust value is calculated using following formula

$$Oi,j(\Delta t) = 10 \times (w1 \times Ci,j(\Delta t) + w2 \times \mathrm{F}\ \mathrm{i,j}(\Delta t))$$

Then the weights are given to first hand and second hand information. The weight is calculated using self adaptive method. It is based on the successful interaction between CHs and a feedback factor whose value between 0 and 1.The weigts is calculated based the following formula.

$$\mathrm{W1}=\frac{\Phi(S)}{\Phi(S)+\Phi(g)} \quad , \quad \mathrm{W2}=\frac{\Phi(g)}{\Phi(g)+\Phi(s)}$$

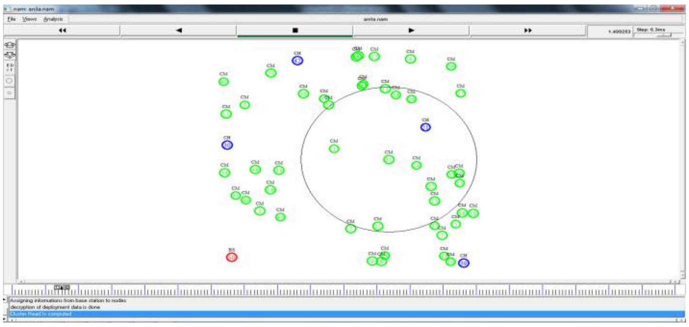
S denote the total amount of successful interactions of CH *i* with *j* during Δ*t*. *g* is the amount of positive feedback ($Ck;j \geq 5$) toward CH *j*.The Φ(*x*) is calculated using the following formula

$$\Phi(S) = 1 - \frac{1}{\alpha + x}$$

Based on the GTD value the decision is made.

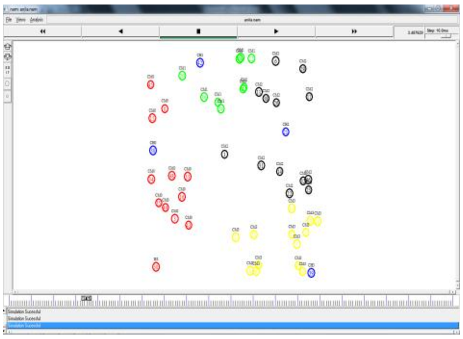
Snapshot

CH Configuration

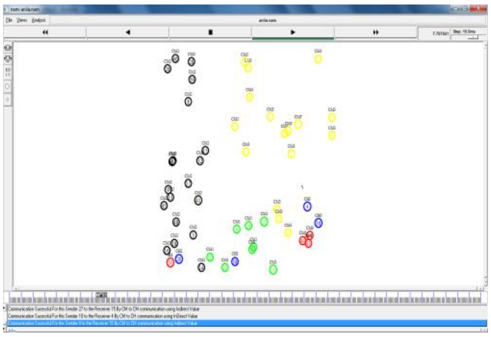


Assigning informations from base station to nodes
decryption of deployment data is done
Cluster Head is computed

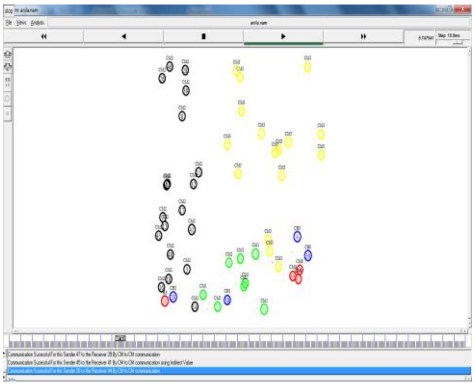
Cluster Member Computed CM - CH && CH-CH Communication



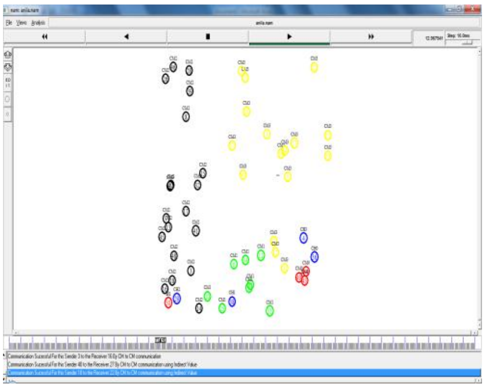
Simulation Sucessful
Simulation Sucessful
Simulation Sucessful



Communication Sucessful For this Sender 27 to the Receiver 15 By CM to CH communication using Indirect Value
Communication Sucessful For this Sender 18 to the Receiver 4 By CM to CH communication using InDirect Value
Communication Sucessful For this Sender 8 to the Receiver 15 By CM to CH communication using Indirect Value



Communication Sucessful For this Sender 47 to the Receiver 39 By CM to CM communication
Communication Sucessful For this Sender 45 to the Receiver 47 By CM to CM communication using Indirect Value
Communication Sucessful For this Sender 35 to the Receiver 44 By CM to CM communication



Communication Sucessful For this Sender 3 to the Receiver 16 By CM to CM communication
Communication Sucessful For this Sender 48 to the Receiver 27 By CM to CM communication using Indirect Value
Communication Sucessful For this Sender 18 to the Receiver 22 By CM to CM communication using Indirect Value

VI. Conclusion And Future Work

This system is the Role based and Energy Efficient Trust system for clustered WSNs. Given the cancellation of feedback between nodes, it can greatly improve system efficiency while reducing the effect of malicious nodes. By adopting a dependability-enhanced trust evaluating approach for cooperations between CHs, it can effectively detect and prevent malicious, selfish, and faulty CHs. It demands less memory and communication overhead as compared with other typical trust systems and is more suitable for clustered WSNs. When the number of CM increases, the communication overhead increases slowly. So in future the communication overhead can be reduced further.

References

[1] D. Kumar, T. C. Aseri, R.B. Patel, EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks, Comput. Commun., Vol. 32, no. 4, pp. 662-667, Apr. 2009

[2] Y. Jin, S. Vural, K. Moessner, R. Tafazolli, An Energy-Efficient Clustering Solution for Wireless Sensor Networks , IEEE Trans. Wireless Comm.. vo. 10, no. 11, pp. 3973-3983, Nov. 2011

[3] O. Younis and S. Fahmy, HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad-Hoc Sensor Networks,IEEE Trans. Mobile Compt., vol. 3, no. 4, pp. 366-379, Oct. 2004.

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

[5] Y. Sun, Z. Han, K. J. Ray Liu, Defense of Trust Management Vulnerabilities in Distributed Networks, IEEE Comm. Mag., Vol.46, No. 2, pp. 112-119, Feb. 2009.