ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

A Reliable Secure Trust Management System in Clustered Wireless Sensor Network

Pradnya Kulkarni, Dr. Arati M. Dixit

M.E Student, Department of Computer, PVPIT, Bavdhan, Pune, Maharashtra, India

Professor, Department of Computer, PVPIT, Bavdhan, Savitribai Phule university of Pune, Pune, Maharashtra, India

ABSTRACT: In Wireless Sensor Network (WSN) consists of distributed autonomous sensors to monitor environmental for physical conditions and it has many practical applications. WSN is of interest for adversaries and they become susceptible to some types in the attacks since they are of deployed in open and to unprotected environments. Due to this limited resources of WSNs, it is challenging to have incorporate basic security features such as for authentication, for key distribution and privacy in WSNs. But, trust in management models the trust on behavior of the elements of networkit can be especially useful for the sensor network environment to enhance the security. Trust management schemes that are for targeted at sensor networks that need to be lightweight in terms of the computational and for communication requirements, so it is powerful in terms of the flexibility in managing between nodes of heterogeneous deployment. This paper surveys different trust management schemes proposed for the wireless sensor network.Security and trust these both are fundamental challenges when it comes to deployment of major wireless sensor networks. In this paper, also author propose a novel hierarchical trust management scheme that it minimizes communication and storage overheads.

KEYWORDS: Trust management, security, wireless sensornetworks, lightweight WSN

I. INTRODUCTION

A WSN is usually made upof a large number of distributed autonomous sensor nodes (SNs) to cooperatively monitor for physical or environmental conditions, though as temperature, sound, vibration, pressure, motion andpollutants. A SN deployed in WSN has the capability to read sensed information and transmitand forward information to base stations a sink node through the multi-hop routing. While SNs have mainly used for various monitoring purposes such as these wild animals, weather, or environments for battlefield surveillance, they have severely resources such as like energy, memory, and computational power. Beyond thisthe wireless environments give more design challenges due to the inherently unreliable communication. The more serious issue is that the nodes may be as compromised and perform malicious attacks such packet dropping and packet modifications to disrupt the normal operations of a WSN where that in SNs usually perform unattended operations. A large number of SNs deployed in WSN also require a scalable algorithm for highly reconfigurable communication.

A WSN contains the battery power sensor nodes with the extraordinarily limited taking care of its capacities. With the slight radio communication extend, sensor node remotely sends messages to base station through the multichip path. The benefits reliability and effectiveness to quality of a trust system these are the most essential necessities in WSNs. Here, existing trust structures made for the clustered WSNs are unequipped for satisfying these requirements because of their high overhead and less dependability. There are several of methods to calculate trust of successive node. The methods include reputation-based trust management, event-based management, collaborative trust management, and agent- dependent trust management. In reputation-based trust management, the node is to stores the number of packet transfers from a node and to calculate the success rate packets transferred from successive node. In this event-based trust management system, the trust rate is too calculated at particular for specific time for events or periodically. In other models, the business models are used for calculate the trust similar no of product for trust management. In agent based trust management systems, the agent node is introduced to store the packet transfer information from cluster of nodes within the communication distance. The agent-based systems relieve the most of processing time of nodes and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

nodes concentrate on transfer of information. Trust-based systems will help to detecting the malicious nodes and to eliminate them from communication path.

Dynamic topology is one of the major property in massive deployment of sensors is dense unknown field. Failures of sensors are common in such situations. The recent research shows that new algorithm for optimal deployment of sensors, localization, energy efficiency, energy aware routing and data aggregation. The algorithms meet the problems of transmission to failure, automatic adjustment in the topology. Further, the task for completion that includes sensing data, reporting data, and detecting malicious node it requires cooperation of neighbor nodes. The cooperation between needs trust of neighboring nodes to research builds on trust of the neighboring nodes and rating successive node that transmits data. Therefore, trust management system that uses limited resources is a requirement. The new trust based system that must detect the malicious node with normal resource usage. This method takes into account directly and indirectly in trust evaluation as well as for energy associated with the sensor nodes in service selection. It also considers the dynamic aspect of trust introducing a trust varying so function which could give the greater weight to the most recently obtained for trust values that are in the trust calculation. The proposed framework is extended to such dynamic mobile inter cluster wireless sensor network environments.

II. LITERATURE SURVEY

Wireless sensor [1]networks (WSNs) in previous years, have shown an ability to observe and interpret the physical world, however, as with every technology, the benefits of WSNs are to establish by significant risk factors and potential. So, someone may ask, that how a user trust the information to provide by the sensor network.
Sensor nodes are small in size and are able to sense,[2] process data, and communicate with each other to transfer the information to the users. Here a typical sensor node developed by researchers at UC Berkeley called Mica2 as presented intypically, a sensor node consists of four sub-systems as.

Computing [3]sub-system that is processor and memory responsible for the control of the sensors and of the execution for communication protocols.
• Communication sub-system transceiver used for to communicate with the neighboring nodes and outside world.
• Sensing subsystem sensor link to the node for the outside world.
• Power supply sub-system that is battery supplies power to the node.
Wireless sensor[4] network consist of sensor nodes with limited no of computation and communication capabilities deployed in large amount that is in tens of thousands as opposed to the tens or hundreds of nodes. Here they present the same challenges so that any other Mobile ad hoc network MANET presents absence of infrastructure, mobility, lack of guaranteed connectivity, but the computation constraint to makes the design for solutions even harder. WSNs have an additional function for the traditional functions of MANETs, which it concerns monitoring events, to collect and process data and transmit sensed information for the interested users. This is to observe difference in the foundation of this new research to model trust in the WSNs.

In recent days,[5] it has been a growing interest in the wireless sensor networks. One of the major and important issues in wireless sensor network is to developing an energy efficient clustering of protocol. Hierarchical clustering of algorithms are very important in the increasing network's life time for each of the clustering algorithm is composed with the two phases, that are setup phase and the steady state phase. The hot point in these algorithms is for the cluster head selection. Here also the impact of heterogeneity of nodes in terms of their energy in wireless sensor networks that isin hierarchically clustered. It assumed that percentage of the population of sensor nodes is for equipped with the additional energy resources. It also assumes that the sensor nodes are randomly distributed over and are not mobile, the coordinates of the sink and the dimensions ofthe sensor field are known. Homogeneous[6][7][8]clustering protocols assume that all the sensor nodes are equipped with the same amount of energy and asresult; they cannot take advantage of the presence of node heterogeneity. Adapting this approach, here introduce energy efficient heterogeneous clusteredscheme for the wireless sensor networks based on the weighted election probabilities of each node so as to become a cluster head according to the residual energy in the each node. Finally, simulation results demonstrate that the proposed heterogeneous clustering approach is more effective for prolonging the network lifetime.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

WSNs [9]technology is relatively new and emerging concept and that has received increasing attention due to the advancement in the wireless communications in the last few years. In addition, to that it need to have very tiny and cheap nodes that being deployed in large numbers and in difficult environments so such as military zones led to increasethe focus by researchers on WSNs. While in wireless communication it is already used in all sectors of daily life routine, WSNs have yet to step beyond the experimental stage. So there is a strong interest in deployment of WSNs in the many applications and for that research effort is significant.

The resource that is efficiency and dependability of trust system should undoubtedly be the most fundamental requirements for the WSN including clustered WSNs. [10]However, existing to trust the systems created for any clustered WSNs are of incapable of satisfying these requirements because of this high overhead and low dependability. A universal trust system for the clustered WSNs for to simultaneous achievement of resource efficiency and the dependability remains lacking.

III. IMPLEMENTATION DETAILS

System Architecture

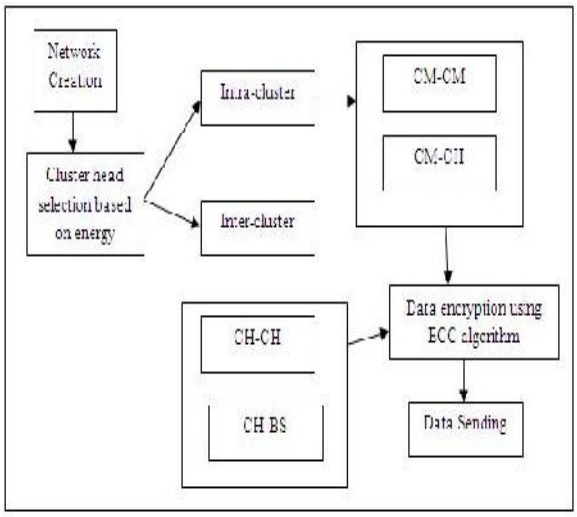

Figure 7.3: System architecture

System Overview

1) Network Topology Model and Assumptions: In network topology, itgenerates network based on energy. In this network contained collection member, cluster head and Base station. To increase the network lifetime itselects the nodes which have high energy as a cluster head. Here cluster head is flexible due to this it stores the network consumption energy. The all cluster member send their equate trust towards the cluster head and all the cluster headtransfer their corresponding trust towards the Basestation.

Trust Decision-Making at CM Level
A CM calculates the trust value of its neighbors based on the
a) Direct trust degree (DTD)
B) Indirect trust degree (ITD)
Direct trust degree (CM-to-CM direct trust) is calculated. On the basis of successful and unsuccessful interactions. Heretwo cluster members communicate with each other. If the onecluster member send the message to the other cluster memberand it receives the acknowledgment within a time period then it is a successful interaction otherwise it is an unsuccessfulinteraction.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

In Indirect trust degree (CM-to-CH direct trust)the communicationoccurs between cluster members to cluster head. Herecluster member sends their corresponding trust value towardsthe cluster head and cluster head store this trust value in matrix.
If any cluster member wants the trust value of others then itasked the feedback to the cluster head and cluster head sendthe positive and negative feedback to the cluster member.

Modules Description

In thiscontribution it proposes three systems
1. Trust System
2. Secure System
3. Trust Secure System

Trust System is LDTS where system calculates trust on the basis of direct and indirect method.
In secure system itprovides the security to the system by implementing ECC algorithm.The ECC algorithm implemented by Secure System that protect to system.The ECC algorithm is adisproportional algorithm. It needs two keys that are
Public and private keys. Public key-based access control schemes are more captivating than proportionate-key based concepts due to high ascendable, low memory necessities,simple key-addition/revocation for a new node. It is a lightweight encryption algorithmbecause it has less key size.
In Trust Secure System itincludes the both methods means it computes the trust system and implement ECC security algorithm.
In GUIitgives three buttons and user can select the technique and execute the project.
At last itcompare the operation on the basis of lightweight and time factor.

Attack	GTMS	LDTS	ECC	Trust Secure
Bad Mounting Attack	X	√	X	√
Garnished Attack	X	√	X	√
Brute Force Attack	X	X	√	√

Table No.1 Attack Table

Algorithm

Elliptic Curve Cryptographic Algorithm

Few terms that will be used,
E! Elliptic Curve
P ! Point on the curve
n! Maximum limit (This should be a prime number)

ECC Algorithm:
The Elliptic Curve Cryptographic(ECC) Algorithm followed by following steps:
1) Alice and Bob Compute edB = S = (S1, S2). (Using Diffie – Hellman Scheme)
Alice sends a message M ε E to Bob as follows:
2)Compute (S1 * S2) mod N = K.
3)Compute K*M = C, and send C to Bob.
Bob receives C and decrypts it as follows:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

4)Compute (S1 * S2)modN = K.
5)Compute (K–1)modN.
(where N = #E)
6)K–1*C = K–1*K*M = M.
In the first method (M1), the sender compute the multiplication between the coordinates of the key in the encryption algorithm, and the receiver compute the multiplication between the coordinates of the key in the decryption algorithm.

Key Generation
Key generation is crucial part where it has to generate both public key andprivate key.After encrypting the message by sender with receiver's public key and private key is decrypt by receiver.
Now, it has to select a number'd' within the range of 'n'.
Using the following equation it can generate the public key
Q = d *P
d = The random number that it has selected within the range of (1 to n-1). Point on the curve is P
'Q' is the public key and 'd' is the private key.

Encryption
Let 'm' be the message it is sending. It has to show this message onthe curve. This has in-depth implementation details. All the greater research on ECCis done by a company called certicom.
Let us assume that 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from[1-(n-1)].Two cipher texts will be generated let it be C1 and C2.
C1 = k*P
C2 = M + k*Q C1 and C2 will be send.

Decryption
To get back the message 'm' that was send to us,
M = C2 - d *C1
M is the original message that hassent.
Proof
How to get the message,
M = C2 - d * C1
'M' can be represented as 'C2 - d *C1'
C2 - d *C1 = (M + k *Q) - d * (k * P)
(C2 = M + k *Q and C1 = k *P)
= M + k *d *P - d *k*P
(canceling out k *d *P)
= M (OriginalMessage)

IV. RESULTS& DISCUSSION

A) Energy

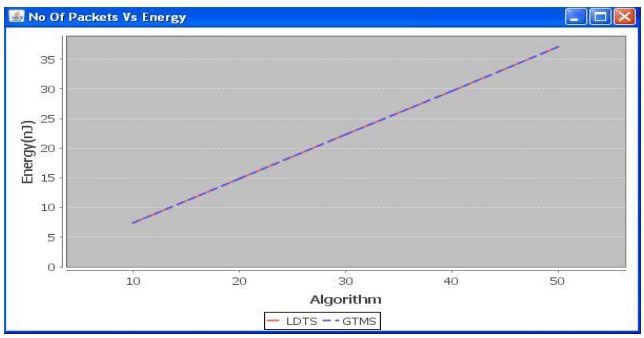

Fig.1 No of Packets Vs Energy

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

In the above given Line Graph it depicts the comparison between No. of packets Vs Energy.On the X-axis shows the Algorithms LDTS and GTMS. On Y-axis it shows an Energy unit in joule where it starts from 0 to 35joules.

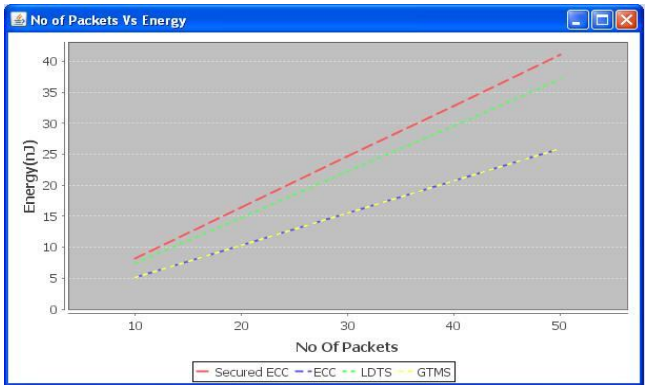

Fig.2 No of Packets Vs Energy

In the above given Line Graph again it depicts the comparison between No. of packets Vs Energy. On the X-axis it has more than two Algorithms Secured ECC, ECC, LDTS and GTMS. On Y-axis it shows an Energy unit in joule where it starts from 0 to 40 joules. In this graph Secured ECC takes more energy to perform operations than remaining algorithms.

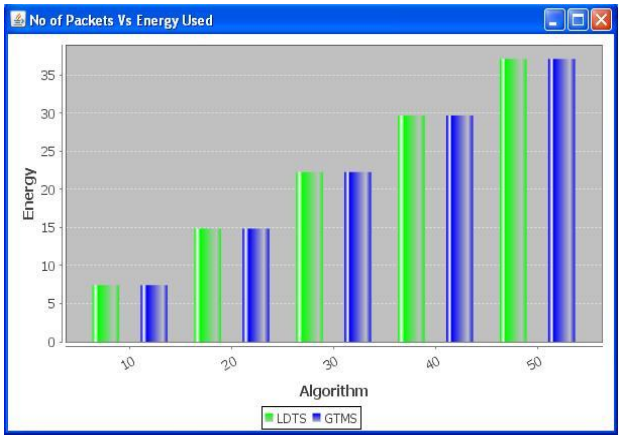

Fig.3 No of Packets Vs Energy Used

In the above given Bar Graph it shows the comparison between No. of Packets Vs Total Energy Used. On the X-axis it has two Algorithms LDTS and GTMS. On Y-axis it shows an Energy unit in joule where it starts from 0 to 35 joules. In this graph GTMS takes more energy to perform operations than LDTS algorithms.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

B) Time

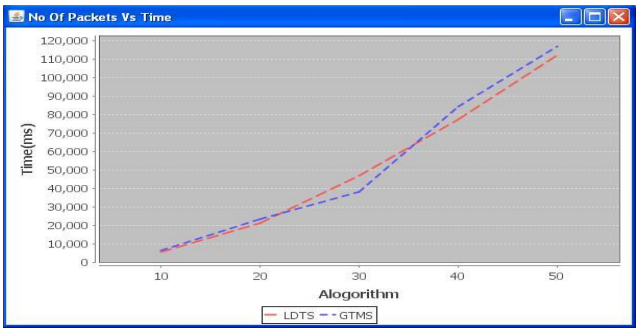

Fig.4 No of Packets Vs Time

In the above given Line Graph it shows the comparison between No. of Packets Vs Total Time. On the X-axis it has two Algorithms LDTS and GTMS. On Y-axis it shows a time in milliseconds where it starts from 0 to 120,000milliseconds. In this graph GTMS takes more time to perform operations than LDTS algorithms.

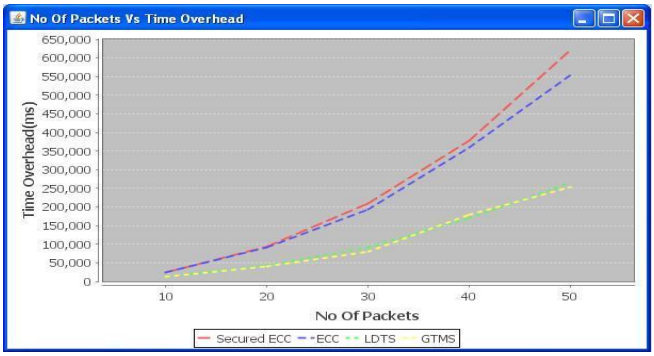

Fig.5 No of Packets Vs Time

In the above given Line Graph again it depicts the comparison between No. of packets Vs Time Overhead. Onthe X-axis more than two Algorithms Secured are exist i.e. ECC, ECC, LDTS and GTMS. On Y-axis it shows Time Overhead in milliseconds where it starts from 0 to 650,000 milliseconds. In this graph Secured ECC takes more time to get execute and perform operations than remaining three algorithms.

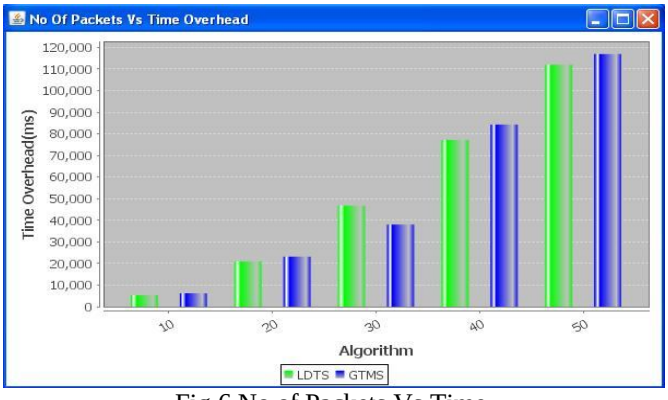

Fig.6 No of Packets Vs Time

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

In the above given Bar Graph it shows the comparison between No. of Packets Vs Total Overhead. On the X-axis there two Algorithms are present i.e. LDTS and GTMS. On Y-axis it shows aTime Overhead in milliseconds where it starts from 0 to 120,000 milliseconds. In this graph GTMS takes more time to perform operations than LDTS algorithms.

V. CONCLUSION

Trust it is an essentialfeature in building relationship between entities that has been studied for long time by scientists from to disparate scientific fields. Every field hasits ownobservedmodeling and calculating trust using different the methods as, one of the most prominent and promising techniques it is the use of statistics, and mainly probabilities to solve the problem, especially in the dynamic networks where topology is changing continuously.

This paper gives brief representationof wireless sensor networks and it challenges related with deploying them in unattended and difficult in environments. It has also initiated the security for problems in WSNs and the need for new innovative approaches to solve these severalissues. In the notion of trust, the difference between trust and its security has been discussed and it explained that trust is not same as security, though they are sometimes used for interchangeably to describe a secure system. The difference between the reputation and trust has also been discussed; the former have only partially affects the latter, which means that based on the reputation, level of trust is based upon an entity.

REFERENCES

1. X. Li, F. Zhou and J. Du, "LDTS: Lightweight And Dependable Trust SystemFor ClusteredWireless Sensor Network", *IEEE Transactions On Informations Forensic and Security, Vo.8, No. 6, June 2013.*
2. P. Raghu Vamsi and Krishna Kant "Systematic Design of Trust Management Systems for Wireless Sensor Networks : A Review", *Fourth International Conference on Advanced Computing Communication Technologies, 2014.*
3. W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "Anapplication-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wireless commun., vol. 1, no. 4, pp. 660-670,Oct. 2002.*
4. S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," *in Proc. 10th ACM Conf. Computer and Comm. Security (CCS'03), 2003, pp. 62-72.*
5. G. Theodorakopoulos and J.S. Basras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE J. Sel. Areas Commun.,vol. 24, no. 2, pp. 318-328, Feb. 2006.*
6. G. V. Crosby, N. Pissinou, and J. Gadze, "A framework for trust-based cluster head election in wireless sensor networks," *in Proc. Second IEEE Workshop on Dependability and Security in Sensor Networks andSystems, 2006,pp. 1022*
7. A.Boukerche, X. Li, and K. EL-Khatib, "Trust based security for wireless ad hoc and sensor networks," *Computer Commun., vol. 30, pp. 24132427, Sep. 2007.*
8. D. Kumar, T. C. Aseri, and R. B. Patel, "EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks," *Comput. Commun., vol. 32, no. 4, pp. 662667, Apr. 2009.*
9. R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. Lee, "Groupbased trust management scheme for clustered wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 11, pp. 16981712, Nov.2009.*
10. F. Bao, I. Chen, M. Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Trans. Netw. Service Mang., vol. 9, no. 2, pp. 169-183, Jun. 2012.*