*International Journal of Application or Innovation in Engineering & Management (IJAIEM)*
**Web Site: www.ijaiem.org Email: editor@ijaiem.org**
**Volume 4, Issue 11, November 2015** **ISSN 2319 - 4847**

# Design of Secure and Trusted Communication in Clustered Wireless Sensor Network

**Madhuri A. Giri [1], Poonam D. Lambhate[2]**

[1] P.G. Student, Dept of Computer Engg, J.S.C.O.E, Hadapsar, Pune, India

[2] Assistance Professor, Dept of Computer Engg, J.S.C.O.E, Hadapsar, Pune, India

## ABSTRACT

***This paper introduces the security and trust concepts in wireless sensor networks and clarifies the difference between them, condition that even though both terms are used interchangeably when defining a secure system, they are not the same. Conventional cryptography methods alone are not adequate for secure routing in Wireless Sensor Networks (WSNs) or the business task in or even the aircrafts utilize, attempting to improve our security. In any case, the wireless sensor networks themselves are partial to security attacks. The trust administration plans include a capable device for the searching of surprising node practices either malicious or faulty. In wireless sensor networks, sensor nodes are the area of investment, must report the cognitive methodology to the sink by sensing, and this report will fulfills the recurrence important of the sink. Inside the network security, divide the thought of trust as an association among substances that manages in distinctive conventions. In wireless sensor network the asset productivity and dependability of a trust system are the most primary requirement. Because of the low dependability and high overhead the created present trust system for wireless sensor networks are not able to satisfying this condition. In this manner there have to present a lightweight and dependable trust system which can proficiently decrease the network utilization while malicious, faulty and selfish cluster heads. This system surpasses the restricts of usual weighting routines for trust factors, in which weights are designated subjectively. Moreover, the result shows that the system demand less correspondence overhead and memory. Also for security use RC4 algorithm.***

**Keywords:** Wireless sensor network, trust management, reputation, trust model, self-adaptivity model and design

## 2. INTRODUCTION

Wireless sensor networks present probability accommodating helpful strategies for distinctive applications including environment and temperature monitoring, freeway movement dissecting, people's heart rates sensing, and various other military applications. An original attributes of these networks is that sensor nodes in networks help each other by transferring data, in network operation and control packets starting with one node then onto the following. It is persistently termed an infrastructure less, self-sorted out, or spontaneous system.

Trust management is essential to perceive malignant, egotistical and traded off nodes which have been approved. It has been comprehensively assumed in several network circumstances, for instance, distributed network, companion and pervasive handling etc. Nevertheless, in all fact, sensor nodes have obliged resources and other unprecedented nature, which make trust management for WSNs more critical and testing. Up to the proposed, verified on the trust management parts of WSNs have primarily centered on nodes' trust evaluation to update the protection and power. The sensible applications of this method fuse the course, data consolidation and cluster head vote.

Clustering algorithms can viably improve the network throughput and adaptability for wireless sensor network like EEHC [5], HEED [4], LEACH, and EC. The nodes are collected into the cluster with the help of cluster algorithm and inside each one cluster the node which has high operation power and energy chose as a cluster head (CH). Generally the nodes closer to the base station will be energetically stacked. Trust establishment in an assembled environment is of extraordinary basics. Trust is the need of one part about the activities of an alternative. A trust design enables a CH to perceive malicious or faulty nodes inside collecting, aides the determination of trusted routing nodes through which a cluster member (CM) can send data to the CH. In the midst of inter-cluster interaction, a trust system moreover helps in the choice of trusted routing gateway nodes or other trusted CHs through which the sender node will forward data to the base station (BS).

A WSN consist of battery-power sensor nodes with unique restricted taking care of capacities. With a slight radio interaction extend, a sensor node remotely sends notification to a base station through a multihop path. The profitable reliability and efficient standard of a trust system are the most important necessities for WSNs. Of course, current trust structures made for clustered WSNs are unequipped for fulfilling these necessities because of their high overhead and low dependability.

Moreover, actualizing complex trust evaluation counts at each CM or CH is not useful. In present trust instruments, trust management framework collected remote criticism and after that the reactions from all the nodes are totaled to get the overall reputation which can be implemented to survey the global trust degree (GTD) of this node. In light of the broadcast nature of the WSN environment, it consists of a considerable number of undependable or malevolent nodes.

Feedback from these undependable nodes may achieve the wrong assessment of criticism. So a trust framework should be specifically reliable the extent that giving organization in an open WSN environment.

## 3. RELATED WORK

In [2] P. Raghu Vamsi and Krishna Kant endeavor to present steps for a precise outline of trust management systems for WSNs. Furthermore, they address the methods emulated by researchers in actualizing trust systems. Besides, they give discussion on state-of-the-art research in planning trust frameworks with synopsis and comparisons.

In [3] make and analyze low-energy adaptive clustering hierarchy (LEACH), a protocol development demonstrating for micro sensor frameworks that solidify the considerations of energy effective cluster based routing and media get to together with application-particular data aggregation to achieve extraordinary execution in regards to structure lifetime, absence of movement, likewise application-saw quality. LEACH joins an alternate, dispersed cluster advancement technique that engages relationship to relationship toward oneself of broad amounts of nodes, algorithms for adjusting clusters additionally turning cluster head positions to evenhandedly convey the energy load among all the nodes, and strategies to enable scattered sign taking care of to extra communications resources.

In [4] Bao et al. (2012) proposed a hierarchical dynamic trust management protocol for cluster-based wireless sensor networks, considering two sections of reliability, to be particular, social trust besides QoS trust. They made a probability model utilizing stochastic Petri nets strategies to dismember the tradition execution; additionally acknowledged subjective trust against target trust got concentrated around ground truth node status.

In EEHC: Energy effective heterogeneous clustered plan for wireless sensor networks by Kumar et al. (2009) [5] proposed an energy efficient heterogeneous cluster plan for wireless sensor networks. The energy efficient moreover effortlessness of association makes EEHC an appealing and healthy protocol for wireless sensor networks. Remembering the finished objective to upgrade the lifetime and execution of the framework network, this paper covers the weighted probability of the choice of cluster heads. In spite of the fact that they contrasted EEHC and LEACH, there are numerous clustering algorithms that they need to look at and there are numerous components that can influence the network lifetime. Further bearings of this study will be managed clustered sensor networks with more than two levels of hierarchy and more than three sorts of nodes.

George Theodorakopoulos and John S. Baras, (2006) [6] concentrate on the trust assessment confirm in ad hoc networks. Trust confirmation may be indeterminate and fragmented because of the ad hoc networks dynamic nature. This plan is totally concentrated around information beginning at the customers of the framework. No bound together system is required, in spite of the way that the region of one can decidedly be utilized. Moreover, customers require not have individual, prompt involvement with one another customer in the framework in order to figure a suspicion about them..

Boukerche et al. [7] proposed ATRM, a novel agent based trust and reputation management plan (ATRM) for wireless sensor networks. Trust and reputation is proposed as a compelling security component for open situations, for example, the Internet, and impressive examination has been carried out on displaying and managing trust and reputation. Utilizing the trust and reputation administration plan to secure wireless sensor networks (WSNs) obliges giving careful consideration to the caused transfer speed and delay overhead, which have been concentrated by most research works. The target of the plan is to oversee trust and reputation provincially with negligible overhead regarding additional messages and time delay

Crosby et al. [8] proposed TCHEM, a conveyed trust-based structure and a system for the vote of trustworthy cluster heads. This mechanism lessens the probability of traded off or malignant nodes from being chosen as cluster heads. TCHEM does not cover trust in subtle element, since various key issues of trust administration are not presented.

In [9] Zhu et al. (2003) portray LEAP (Localized Encryption and Authentication Protocol), a key administration Protocol for sensor networks that is expected to support in-network preparing, while meanwhile limiting the security impact of a node trade off to the quick framework neighborhood of the compromise node. The framework of the convention is roused by the discernment that unique sorts of messages exchanged between sensor nodes have differing security requirements, and that a lone keying segment is definitely not suitable for social affair these assorted security necessities.

## 4. IMPLEMENTATION DETAILS

### 3.5 System Overview

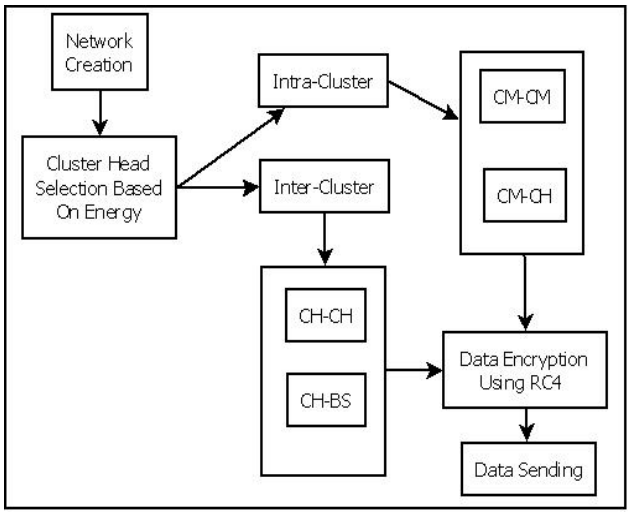


**Figure 1** System Architecture

**1. Network Topology Model and Assumptions**

In network topology, we create network on the basis of energy. In this network contained Cluster member, cluster head and Base station. To increase the network lifetime we select the nodes which have high energy as a cluster head. Here cluster head is dynamic due to this it saves the network consumption energy. The all cluster member send their corresponding trust towards the cluster head and all the cluster head transfer their corresponding trust towards the Base station.

**2. Lightweight Scheme for Trust Decision Making [1]**

LDTS (A lightweight and dependable trust system) make easy trust decision making based on a lightweight scheme. This scheme is discuss in below:

**A. 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. Here two cluster members communicate with each other. If the one cluster member send the message to the other cluster member and it receives the acknowledgment within a time period then it is a successful interactions otherwise it is an unsuccessful interactions.

In Indirect trust degree (CM-to-CH direct trust) the communication occurs between cluster members to cluster head. Here cluster member sends their corresponding trust value towards the cluster head and cluster head store this trust value in matrix. If any cluster member wants the trust value of others then it asked the feedback to the cluster head and cluster head send the positive and negative feedback to the cluster member.

**B.Trust Decision-Making at CH Level [1]**

The selection of CHs is a very important step for dependable communication. In LDTS, the GTD of a CH is evaluated by two information sources

a) CH-to-CH direct trust and

b) BS-to-CH feedback trust.

Direct trust degree (CH-to-CH direct trust) is calculated on the basis of successful and unsuccessful interactions. Here two cluster heads communicate with each other. If the one cluster head send the message to the other cluster head and it receives the acknowledgment within a time period then it is a successful interactions otherwise it is an unsuccessful interactions.

In Indirect trust degree (CH-to-BS direct trust) the communication occurs between cluster head to base station. Here cluster head sends their corresponding trust value towards the base station and base station store this trust value in matrix. If any cluster head wants the trust value of others then it asked the feedback to the base station and base station send the positive and negative feedback to the cluster head.

**C.Self adaptive weighting method [1]**

In this method weights are assigned subjectively. Here global trust degree is calculated on the basis of direct and indirect weighting method which is calculated using successful interactions and positive feedbacks.

**D.Secure trust system**

It is feasible for an attacker to change the trust values. Consequently it is fundamental that the trust values ought to be passed secure. The data packets likewise need to be encoded amid transmission with the goal that the transitional nodes are not ready to view the information amid transmission. For encryption methodology, considering the energy requirements of WSNs, These new designs and other particular features (e.g., autonomous of any particular routing schemes and platform et cetera) on the whole makes the configuration a lightweight, self-adaptive, and trustworthy arrangement that can be utilized as a part of any clustered WSN.

**E.Attacks**

1. **Garnished Attack: -** In this attack, malicious node behaves well and badly alternatively with the aim of remaining undetected while causing damage. Sometimes they provide successful interactions and unsuccessful interactions. For instance garnished malicious nodes may suddenly conduct attacks as they accumulate higher trustworthiness.
2. **Bad Mounting Attack: -** In this attack, as long as feedback is considered, malicious nodes considered malicious nodes can provide dishonest feedback to frame good parties and/or boost trust values of malicious nodes.

### 3.6 Algorithm

**1. RC4 algorithm**

Rc4 is presumably the most generally utilized stream cipher as a part of the world because of its straightforwardness and proficiency.

PRGA (P)
Initialization
i←0
j←0
Generation loop:
i←(i+1)mod256
j←(j+S[i])mod256
P[i]↔P[j]
Output z ←+P[P[i]+P[j]mod256]
IPRGA(P,i,j)
Generation loop:
P[i]↔P[j]
j←(j-P[i]+256)mod256
i←(i-1+256)mod256
Output z←P [(P[i] + P[j]) mod256]

### 3.7 Mathematical Model

**1. Direct Trust for Intra-cluster**

$$T_{x,y} = \left[\left(\frac{10 \times s_{x,y}(\Delta t)}{s_{x,y}(\Delta t) + u_{x,y}(\Delta t)}\right)\left(\frac{1}{\sqrt{u_{x,y}(\Delta t)}}\right)\right]$$

Where, $T_{x,y}$ is an Intra-Cluster Trust
$s_{x,y}(\Delta t)$ is a successful interactions between Source x and Destination y in ($\Delta t$) i.e. time
$u_{x,y}(\Delta t)$is a successful interactions between Source x and Destination y in ($\Delta t$) i.e. time

**2. Direct Trust for Inter-Cluster**

$$C_{i,j} = \left[\left(\frac{10 \times S_{i,j}(\Delta t)}{S_{i,j}(\Delta t) + U_{i,j}(\Delta t)}\right)\left(\frac{1}{\sqrt{U_{i,j}(\Delta t)}}\right)\right]$$

Where, $C_{i,j}$ is a Inter-Cluster Trust
$S_{i,j}(\Delta t)$ is a successful interactions between Source i and Destination j in ($\Delta t$) i.e. time.
$U_{i,j}(\Delta t)$ is a unsuccessful interactions between Source i and Destination j in ($\Delta t$) i.e. time.

**3. Indirect Trust for Intra-Cluster**

$$R_{ch,y}((\Delta t) = \lceil 10 \times E(\phi(p|r,v))\rceil$$

Where,

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

Where, r is number of positive feedbacks and v is number of negative feedbacks.

**4. Indirect Trust for Inter-Cluster**

$$F_{bs,j}(\Delta t) = \left\lceil \frac{10 \times E\left(\varphi(p|g,l)\right) + \overline{C_{k,j}}(\Delta t)}{2} \right\rceil$$

Where,

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

g is the number of positive feedbacks and
l is the number of negative feedbacks

## 5. RESULT AND ANALYSIS

The following figure shows the result of the system.
Figure 2 shows the cluster formation. We form the 4 cluster for intra cluster and inter cluster communication.

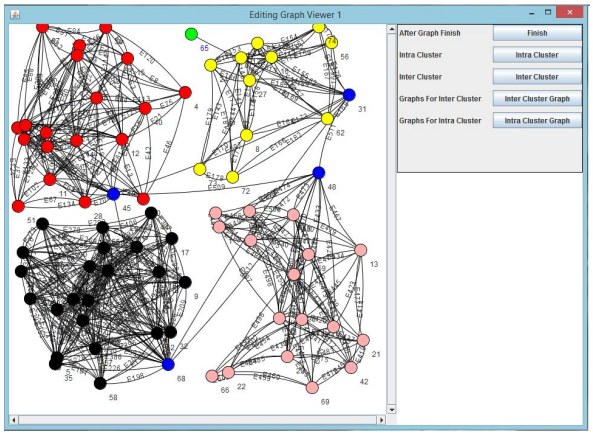


**Figure 2** Cluster Formation

Figure 3 shows the Intra cluster communication. In intra cluster communication we can take the source and destination in the same cluster for data transfer; means CM to CM trust calculation can be done.

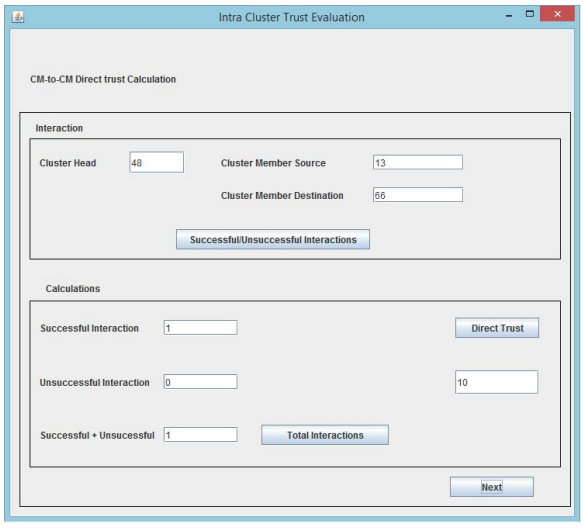


**Figure 3** Intra Cluster Trust Calculations

Figure 4 shows the Inter cluster communication; in this we can take two different cluster head and source from first cluster head and destination from another cluster head; means CH to CH trust calculation is done.

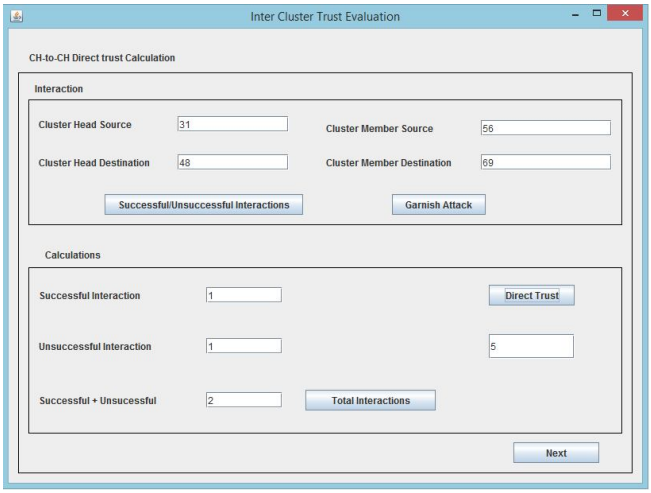


**Figure 4** Inter Cluster Trust Calculation

The analysis graphs are shown in the following figure

The following graph depicts the Intra cluster operation in Packet Dropping, On the X-axis there are two bars are shown i.e. normal data sending and secure data sending. On the Y-axis the No. of packets drops is shown, it starts from 0 to no. of packets drops. Normal data sending bar goes at the top means packet drop ratio is high in normal data sending and packet drop ratio goes low in secure data sending using encryption with RC4 algorithm.

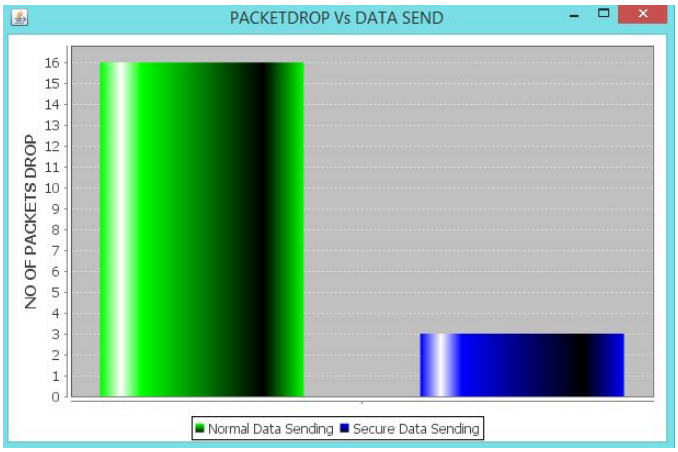


**Figure 5** Intra cluster Graph

The following graph depicts the Inter cluster operation in Packet Dropping, On the X-axis there are two bars are shown i.e. normal data sending and secure data sending. On the Y-axis the No. of packets drops is shown, it starts from 0 to no. of packets drop. Normal data sending bar goes at the top means packet drop ratio is high in normal data sending and packet drop ratio goes low in secure data sending using encryption with RC4 algorithm.

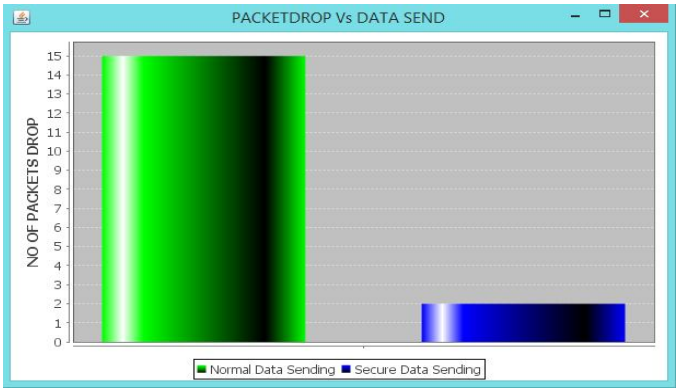


**Figure 6** Inter cluster Graph

## 6. CONCLUSION AND FEATURE SCOPE

This model can uniquely enhance system efficiency while diminishing the impact of malicious nodes. By embracing a reliability enhanced trust assessing methodology for collaborations between CHs, lightweight trust system can adequately identified and avoid malicious, selfish, and flawed CHs. Because of wiping out criticism between cluster members (CMs) or between cluster heads (CHs), this technique can importantly progress system efficient while decreasing the impact of malicious nodes. The present secure protocol can be utilized as a broadcast and multi-throwing. It also save the energy of a nodes and grow the lifetime of a network because here the cluster heads are change based on the energy. And also provide the security by encrypting the data and trust values. To encrypt the data for secure data sending, we use RC4 algorithm for encryption in the system.

## References

[1] A. X. Li, F. Zhou and J. Du, "LDTS: Lightweight and Dependable Trust System for Clustered Wireless Sensor Network", IEEE Transactions On Information 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, "An application-specific protocol architecture for wireless microsensor networks," IEEE Trans. Wireless communication., vol. 1, no. 4, pp. 660-670,Oct. 2002.
[4] 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.
[5] 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.
[6] 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.
[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] 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 and Systems, 2006,pp. 1022.
[9] 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.
[10] 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.
[11] Z. Liang and W. Shi, "TRECON: A trust-based economic framework for efficient internet routing," IEEE Trans. Syst., Man, Cybern. A, Syst., Humans, vol. 40, no. 1, pp. 52-67, Jan. 2010.

**AUTHOR**

**Madhuri A. Giri,** Student of ME Computer Engineering, Jayawantrao Sawant College of Engineering, Hadapsar, Pune University, India**.**