Lightweight Cluster Head Election (LCHE) Based on Trust System for Clustered Wireless Sensor Network

[1]Prof.Sharmila Arun Chopade, [2]Prof.Rupali Pravin Adhau
[1]Assistant Professor, [2] Assistant Professor
[1]Computer Department,
[1]DYPIET,Ambi, Pune, India.

Abstrac : Trust is defined as the level of confidence in a thing or a person, it is important in Wireless sensor network (WSN) .Traditional trust management developed for WSNs are incapable of satisfying requirements such as resource efficiency and dependability of a trusted system, due to their high overhead and low dependability, most fundamental requirements of any wireless sensor networks (WSN) are resource efficiency and dependability. The election of a malicious node at the cluster head is one of the most significant violation in clustered WSN. In this work, The proposed a Lightweight Cluster Head Election Based on Trust System for clustered Wireless Sensor Network for WSNs, A lightweight trust evaluating scheme for cooperation between CM (Cluster Member) or between CHs(Cluster Head). 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 bad-mounting attacks by compromised CM and election for cluster head election. CH election is a necessary process in the cluster based networks. Many parameters can consider for electing a cluster head such as trust, location, mobility, energy, throughput etc.

IndexTerms - Resource Efficiency;Trust Management;Wireless Sensor Networks(WSNs).

I. INTRODUCTION

Trust is defined as the level of confidence in a thing or a person. Various engineering models such as reliability, security, availability, usability, safety, and privacy models incorporate some limited aspects of trust with different meanings. Trust in a network gives many benefits such as it solves the problem of providing corresponding access control based on the quality of SNs, solves the problem of providing reliable and it makes the traditional security services. Traditional trust management systems have not considered the trust value of cluster head, in traditional system they are considered the cluster head, which having high computational power but only computational power is not sufficient for deciding cluster head, some case cluster head having high computational power may be malicious. A lightweight trust calculating scheme for clustered WSN, evaluation of cooperation between the seams or between CHs, the indirect trust of a CMs is evaluated by its CH. Thus, each CM does not need to maintain the feedback from other CMs, which will reduce the communication overhead. The feedback of a CH is applied a similar manner to obtain the same benefits. A dependability-enhanced trust evaluating approach of co-operations between CHs. Considering that CHs take on large amounts of data forwarding and communication tasks, this trust evaluating approach have defined for cooperation between CHs. LCHE approach can effectively reduce networking consumption while preventing malicious, selfish, and faulty CHs.

The proposed algorithm improves the packet delivery ratio, resource efficiency, dependability. Further paper is organized as follows section 2 generalized architecture of protocol and followed by related work. The architecture of the proposed system is presented in section 3. The work in progress is presented in section 4 and finally conclusion and future work is in section 5.

II. LITERATURE SURVEY

Wireless sensor networks (WSNs) goal is to secure the network against all sorts of attacks, such as fabrication, injection, eavesdropping, impersonation and modification of packets, Sensor node issues are accountable, privacy, availability, data authentication and data integrity. The previous trusts system for wireless sensor network are GTMS [2], ATRM [10],HTMS [3], LDTS [8] but this system having some limitation on resource efficiency and are not focused on trusted cluster head election.

A. Hybrid Trust Management System(HTMS)

The hybrid trust management frameworks accept, Combine different types of trust evidence, and have properties of both certicate-based and behaviour based approaches. Behaviour based trust management scheme based on node behaviour. [3]

B. Group-Based Trust Management Scheme (GTMS)

Riaz Ahmed Shaikh has proposed an GTMS [2] scheme GTMS that calculates the trust value based on two types i.e. direct or indirect observations. Direct observations represent the number of successful and unsuccessful communication and indirect observations represent the recommendations of trusted peers about a specific node. Here, interaction means the cooperation of two nodes. GTMS evaluates the trust of a group of nodes in contrast to traditional trust schemes that always focuses on the trust values of individual nodes. GTMS gives WSN the benefit of requirement of less memory to store trust records at each node. GTMS aids in the significant education of the cost associated with the trust evaluation of distant nodes. However, GTMS relies on a broadcast based strategy to collect feedback from the CMs of a cluster, which requires a significant amount of resources and power. [2]

C. Agent-Based Trust and Reputation Management (ATRM)

Boukerche has proposed an ATRM [10] scheme for WSN, Which is based on a clustered WSN and calculates trust in a fully distributed manner. ATRM scheme requires an agent based platform, and it assumes that there is a single trusted authority; this is responsible for generating and launching mobile agents, which makes it vulnerable against. ATRM also assumes that mobile agents are resilient against malicious nodes that try to steal or modify information carried by the agent. In many applications, this assumption may not be realistic. Therefore, these works are not well suited for realistic WSN applications. [10]

III. IMPLEMENTATION DETAILS

A. Design

The research objective of the proposed work is to reduce Communication overhead, reduce storage overhead, and improve packet delivery ratio and build strong trust system along with lower energy consumption.

B. System Overview

[1] system diagram is a specialized, high-level type of flowchart. Its highly structured form presents a quick overview of major process steps and key process participants, as well as the relationships and interfaces involved. The architecture of the system is shown in Fig 1.

LCHE using two type of trust calculation method, direct and indirect trust calculation. Direct trust calculation method calculates trust based on successful and unsuccessful transition. Indirect calculates trust based on feedback of other nodes in cluster, Direct trust calculation are used to calculates trust value of cluster members to cluster members (CM to CM) and cluster head to cluster head (CH to CH) .Indirect trust calculation are used to calculates trust value of cluster head to cluster members (CH to CM) and Base station to cluster head (BS to CH) . LECH select best cluster head on trust value.

Analysis shows that will select the cluster head, which is the trusty and healthy. LCHE select trusted cluster head which increase packet delivery ratio and throughput as shown in Fig.1

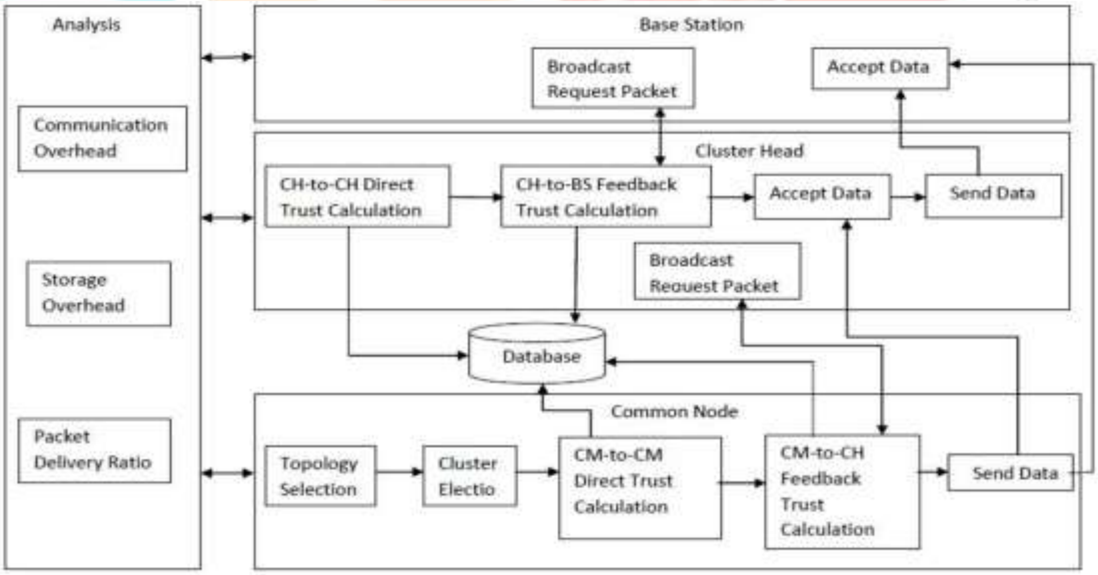

Fig. 1: Block diagram

C. Trust calculation mechanism

1. CM-to-CM Direct Trust Calculation: CM-to-CM Direct Trust Calculated by using equation (1)

$$C_{i,j}(\nabla t) = \left[\left(\frac{10*S_{i,j}\,(\nabla t)}{S_{i,j}\,(\nabla t)+U_{i,j}(\nabla t)} \right) \left(\frac{1}{\sqrt{U_{x,y}(\nabla t)}} \right) \right] [1]$$

Where∇t is a window of time and i,j are the cluster member. The length (∇t) could be made shorter or longer based on network analysis scenarios. Thus, as time elapses, the window forgets old experiences, but adds newer experiences. S(i,j)(∇t) is the total number of successful interactions of node x with y during time∇t, U(i,j) (∇t) is the total number of successful interactions of node i with j during time∇t , T(i,j)(∇t) is CM-to-CM direct trust.

2.CH-to-CM Feedback Trust Calculation:

Supposing the existence of (n-1) CMs in a cluster. The cluster head CH will periodically broadcast the request packet within the cluster. In response, all CMs in the cluster will forward their trust values toward other CHs. Then, CH will maintain these trust values in a matrix H,

$$H = \begin{pmatrix} T_{1,1} & \cdots & T_{1,n-1} \\ \vdots & \ddots & \vdots \\ T_{n-1,1} & \cdots & T_{n-1,n-1} \end{pmatrix} \textbf{[2]}$$

3. *CH-to-CH Direct Trust Calculation:* CH-to-CH Direct Trust Calculated by using equation.

$$T_{x,y}(\nabla t) = \left[\left(\frac{10 * s_{x,y}\ (\nabla t)}{s_{x,y}\ (\nabla t) + u_{x,y}(\nabla t)} \right) \left(\frac{1}{\sqrt{u_{x,y}(\nabla t)}} \right) \right] [3]$$

Where∇t is a window of time and x,y are the cluster head(CH). The length ∇t) could be made shorter or longer based on network analysis scenarios. Thus, as time elapses, the window forgets old experiences, but adds newer experiences. S(x,y) (∇t) is the total number of successful interactions of node x with y during time∇t), U(x,y) ∇t) is the total number of successful interactions of node x with y during time(∇t) . T(x,y)(∇t) is CH-to-CH direct trust.

4 . *BS-to-CH Feedback Trust Calculation*:

Supposing the existence of (n-1) CHs in a cluster. The cluster head ch will periodically broadcast the request packet within the cluster. In response, all CMs in the cluster will forward their trust values toward other CMs to . Then, ch will maintain these trust values in a matrix H ,

$$H = \begin{pmatrix} C_{1,1} & \cdots & C_{1,m} \\ \vdots & \ddots & \vdots \\ C_{m,1} & \cdots & C_{m,m} \end{pmatrix} [4]$$

5. *Cluster head election*

The cluster head performs the usual functions such as data fusion, aggregation and higher level transmission to the base station. The self-election for the first sets of cluster-heads. This is consistent with our initial assumption that there are no malicious nodes at setup. The cluster head schedules the transmission of each member and inform all the members when the clusters are established. The current cluster heads computational power level falls below a predetermined threshold; it broadcasts a new election message within the cluster.

All the nodes, then vote for a new cluster head using confidential message. This is done by replying to the new election message with its choice of node. The reply is encrypted with the pairwise key with the cluster head. Neighboring nodes have no idea of the political affiliation of each other since the key is Private and, different for each node cluster head pair. The top pick from its list of trusted neighbors is selected as the nodes candidate. The current cluster head, then tallies the votes and decides the winner based on max number of votes. The node with the second highest number of votes is selected as the vice cluster head. At the completion of the election, the cluster head multicast the winner to all the members of the cluster. The new winner and have to pass a challenge-response from the cluster head before they are allowed to take up the charge as CH. If it fail incumbent CH informs the cluster members and initiate a new election for the replacement of the corrupt node(s), which we define here as the nodes that did not pass the challenge-response. The malicious node(s) are added in the blacklist cluster nodes and set trust value -1. The CH will broadcast a not trusted message. In this case, nodes select the least trusted neighbor node and reply to the CH by the voting process.

The CH check the no trust messages and selects the node that is least trusted by the most nodes. That node is then given a challenge response.

3.2.2. Algorithm

A cluster head election based on trust value.

```
1) If  the CP level () <= threshold or CH duration >=predetermined time
2)  NElection( )
3) broadcast election()
4) incount node()
5) If Tie
6) Top node= randomly selects node ()
7) Else
8) top node= max count ()
```

```
9) EndIf
10) Send challenge response to the top node
11) If challenge response () =pass
12) new head = top node
13) Broadcast new head
14) Else
15) blacklisted=top node
16) Broadcast blacklisted
17) NElection ()
18) EndIf
19) End
```

IV. RESULTS AND DISCUSSION

A. Result

The metrics used to store trust value which in evaluated By using a direct trust calculation method and using feedback methods. Trust database stored in the matrix.

B.Result set

The trust evaluation in terms of resource effectiveness and attendance is as follows:

1) Storage overhead of the trust database at CH node.

2) Storage overhead of the trust database at CM node.

3) Trust evaluation at each CM and CH.

Select cluster head based on trust value. *C. Simulation Results*

Results are shown in Fig 2, Fig 3&Fig4. Energy graph shown Fig 2 & Packet Delivery Ratio shown in Fig3 .Fig 2 show that Energy level of proposed system is high as compare to old trust system. LCHE change cluster head when CH energy level goes below threshold value. LCHE select trusted cluster head which increase packet delivery ratio and throughput also as show in fig3 & fig4

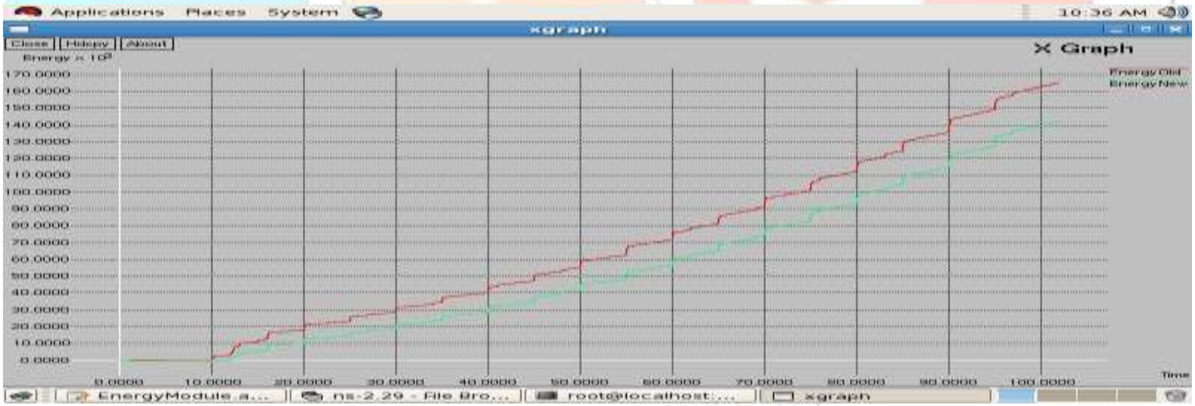

Fig. 2: Energy Graph

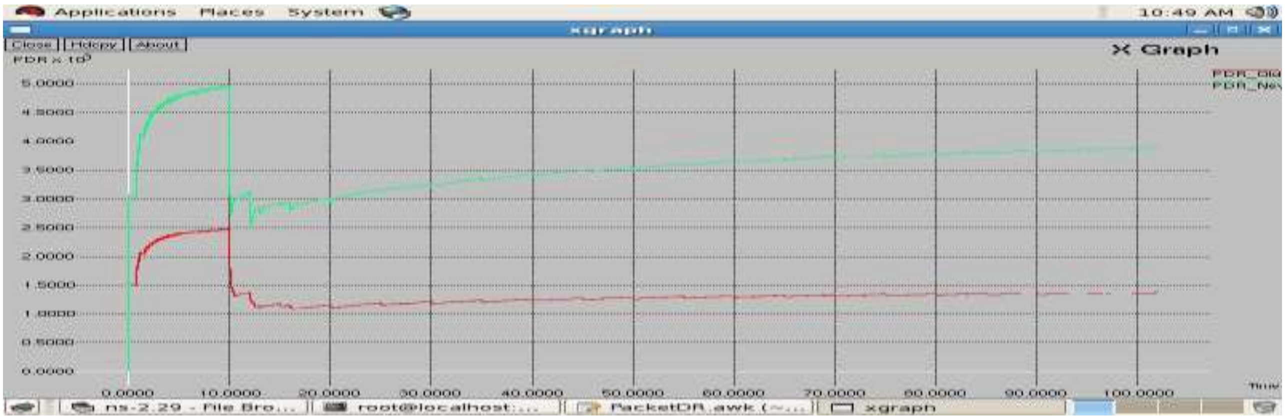

Fig. 3: Packet Delivery Ratio

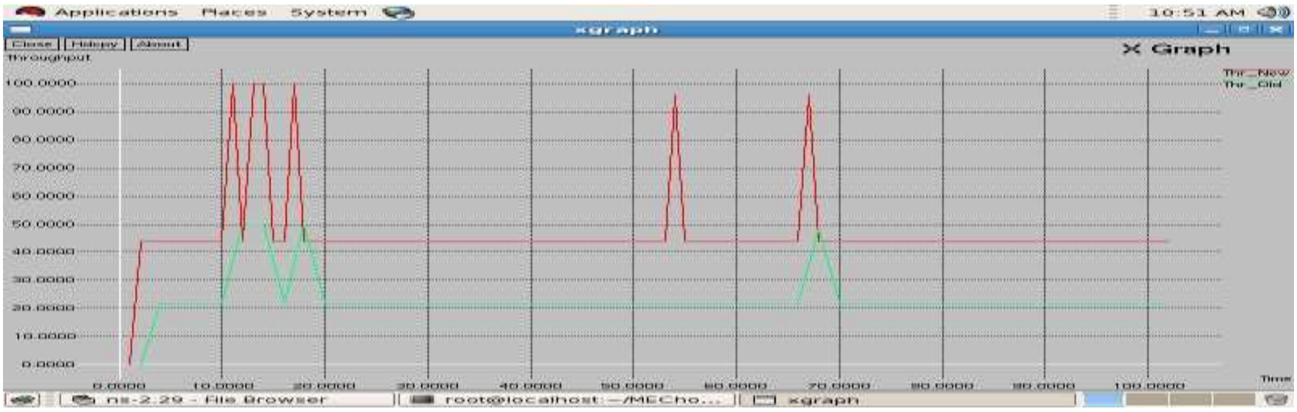

Fig. 4: Throughput

V. CONCLUSION

Lightweight Cluster Head Election (LCHE) Based on Trust System for clustered Wireless Sensor Network improves the dependability between CM and CH and reduces the communication overhead within the cluster. By using LCHE we will select the cluster head, which is the trusty and healthy. LCHE is resource efficient based practical and theoretical analysis.

V. ACKNOWLEDGMENT

The authors would like thanks to the publishers, researchers for making their resources available and teachers for their guidance. we also thank the collage authority for providing the required infrastructure support. Finally, we would like to extend a heartfelt gratitude to frriends, family member.

REFERENCES

[1] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, A survey of trust and reputation management systems in wireless communications in Proc. IEEE, vol. 98, no. 10, pp. 175217754, Oct. 2010.

[2] R. A. Shaikh, H. Jameel, B. J. d Auriol, H. Lee, and S. Lee, Group-based trust management scheme for clustered wireless sensor networks in IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 11, pp. 16981712, Nov. 2009.

[3] E. Aivaloglou and S. Gritzalis, H ybrid trust and reputation management for sensor networks in Wireless Netw., vol. 16, no. 5, pp. 14931510, Jul.2010

[4] Y. Sun, Z. Han, and K. J. R . Liu, Defense of trust management vulnerabilities in distributed net works, in IEEE Commun.Mag., vol. 46, no. 2, pp. 112119, Feb.2009. S. Ganeriwal, L. K. Balzano, and M. B. Srivastava. Reputation-based framework for high integrity sensor networks. In ACM Trans. Sensor Netw, May 2008.

[5] A. Boukerche, X. Li, and K. EL-Khatib, Trust-based security for wireless In ad hoc and sensor n etworks, Computer Commun., vol. 30,24132427, Sep. 2007.

[6] R. Ferdous, V. Muthukkumara samy, and E. Sithirasenan, Trust-based cluster head selection algorithm for mobile ad hoc networks in in Proc. 2011 Int. Joint Conf. IEEE TrustCom-1111/IEEE ICESS-11/FCST-11,589596.

[7] Xiaoyong Li, Feng Zhou, an d Junping Du, A Lightweight and Dependable Trust System for C lustered Wireless Sensor Networks in IEEE transactions on informatio n forensics and security, vol. 8, no. 6, june 2013.

[8] S. Ganeriwal and M. B. Srivas tava, Reputation-based framework for high integrity sensor networks i n Proc. ACM Workshop Security of ad hocand Sensor Networks (SASN04), Oct. 2004, pp. 6667.

[9] Yenumula B. Reddy, Trust-B ased Approach in Wireless Sensor Networks Using an Agent To Each Cluster inInternational Journal of Security,Privacy and Trust Management (IJSPTM), Vol.1, No.1, February 2012

[10] A.Rezgui M. Eltoweissy, Areliable adaptive service driven efficient routing protocol suite for sensor -actuator networks IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 5, pp. 607622, May 2009.

[11] G. V. Crosby, N. Pissinou, and J. Gadze, A framework for trust-based cluster head election in wireless sensor networks in Proc. 2011 Int. Joint Conf. IEEE TrustCom-1111/IEEE ICESS-11/FCST-11, pp. 589596.