© 2018 IJSRSET | Volume 4 | Issue 8 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Secure, Reliable and Lightweight Trust System Which Enhance Security and Energy Efficiency of Wireless Network System

Alka V. Phadatare, N. P. Chawande

Department of Computer Engineering, A. C. Patil College of Engineering, Kharghar, Navi Mumbai, Maharashtra, India

ABSTRACT

In WSN, sensor nodes is the centre of interest which report the cognitive process to the sink by sensing the data, and this report will satisfies the report frequency necessary by the sink. Inside the domain of system security, system deciphers the idea of trust as a connection among entities that take part in different conventions. Trust relations are focused around confirmation made by the past connections of substances inside a convention. In wireless sensor network the resource efficiency and reliability of a trust system are the most basic supplies. Due to the low reliability and high overhead the developed existing trust systems for wireless sensor networks are unable of satisfying these supplies. Therefore there is need to propose a lightweight and reliable trust system which can efficiently decrease the networking consumption while malicious and faulty cluster heads and also exceeds the limitations of traditional weighting methods for trust factors in which weights are allocated subjectively and also insist less communication overhead and memory. In contribution if attack is found in CH then cluster members transfer data to the DCN. Also in this system introduced the method DCN share data with the clusters DCN in tree structure. If attack is found in Data Collection Node (DCN) then Base Station recovered the data from other DCN and prevents data loss. Also in proposed system we used ECH algorithm for clustering process. Due to this system can forward data securely and efficiently and improve the accuracy of the network and minimize the data loss.

Keywords: Data collection node, base station, wireless sensor network, trust management.

I. INTRODUCTION

Wireless sensor systems propose conceivably helpful arrangements for different applications including atmosphere and temperature observing, freeway traffic analyzing, individuals heart rates sensing, and numerous other military applications. A real feature of these systems is that sensor nodes in systems help one another by passing information, in network process and control packets starting with one node then onto the next. It is regularly termed an infrastructureless, self-organized, or spontaneous system. Trust management is major to recognize pernicious, selfish and compromised nodes which have been validated. It has been broadly contemplated in numerous network situations, for example, peer-to-peer network, peer and pervasive processing et cetera. Be that as it may, in all actuality, sensor nodes have constrained assets and other extraordinary characters, which make trust management for WSNs more critical and testing. Up to the present, explore on the trust management components of WSNs have mainly focused on nodes trust assessment to upgrade the security and power. The reasonable applicationsof this strategy incorporate the course, information incorporation and cluster head vote. Clustering algorithms can effectively improve the network throughput and scalability for wireless sensor network like EEHC, HEED , LEACH [4] , and EC [13]. The nodes are grouped into the cluster with the help of clustering algorithm and within each cluster the node which have high computing power and energy selected as a cluster head CH).Typically the nodes closer to the base station will be vigorously loaded.[7] Trust foundation in a grouped environment is of incredible criticalness. Trust is the sender node will forward information to the base station (BS). A WSN contains battery-power sensor nodes with greatly restricted handling abilities. With a thin radio communication range, a sensor node remotely sends messages to a base station through a multi-hop path. The asset effectiveness and reliability of a trust framework are the most basic necessities for WSNs. Then again, existing trust frameworks created for clustered WSNs are unequipped for fulfilling these necessities due to their high overhead and low reliability. Additionally, implementing complex trust assessment calculations at every CM or CH is not practical. In existing trust mechanisms, trust management system gather remote feedback and then the criticisms from all the nodes are aggregated to get the worldwide notoriety which can be utilized to assess the global trust degree (GTD) of this node. Because of the broadcast nature of the WSN environment, it contains a substantial number of undependable or malicious nodes. Criticism from these undependable nodes may bring about the incorrect evaluation of feedback. So a trust system ought to be profoundly reliable as far as giving administration in an open WSN environment.[10]

The system consists of:

- This approach facilitates trust decision making based on a lightweight scheme. This model can greatly improve system efficiency while reducing the effect of malicious nodes. the desire of one element about the activities of an alternate. A trust framework empowers a CH to recogni e faulty or malicious nodes inside a group, guides the selection of trusted routing nodes through which a cluster member (CM) can send information to the CH. Amid inter-cluster communication, a trust framework additionally helps in the selection of trusted routing gateway nodes or other trusted CHs through which
- If attack is found in DCN then Base Station recovered data from other DCNs.
- If attack is found on CH then cluster member send data to the DCN i.e. data collection node and DCN forward data to the other DCN and base station in tree structure.
- If attack is found on Data Collection Node (DCN) then Base Station recovered the data from other data collection nodes (DCNs).
- For cluster formation ECH algorithm is implemented.
- Due to this, system can minimize the data loss and forward data securely and efficiently.

II. LITERATURE SURVEY

This approach gives them the benefit of requiring less memory to store trust records at each Sensor node in the network. GTMS works on two topologies: intragroup topology where distributed trust management approach is used and intergroup topology where centralized trust management approach is adopted. This methodology helps to drastically reduce the cost associated with trust evaluation of distant nodes. GTMS not only provides a mechanism to detect malicious nodes but also provides some degree of prevention mechanism. [9]

This trust scheme consider not only quality of service (QoS) trust derived from communication networks, but also social trust derived from social networks to judge if a node is trustworthy to deal with selfish (uncooperative) or malicious nodes. This approach design and validate a hierarchical trust management protocol that can dynamically learn from past experiences and adapt to changing environment conditions (e.g., increasing hostility or misbehaving node population) to maximize application performance and enhance operation agility. This is achieved by addressing critical issues of hierarchical trust management, namely, trust composition, aggregation, and formation. For trust composition, novel social and Quality of Service trust components are considered. For trust aggregation, the best way to aggregate trust (direct vs. indirect trust evaluation) and propagate trust (trust data collection, dissemination and analysis) for each individual trust component, and ascertain protocol accuracy by means of a novel model-based analysis methodology.[1]

This framework is useful for cluster-based wireless sensor networks and, a mechanism that reduces the likelihood of compromised or malicious nodes being selected (or elected) as cluster heads. Number of assumptions are made. Initially, a reliable link layer protocol and cluster formation algorithm is assumed.[12]Once the clusters are formed they maintain the same members, except for cases where nodes are blacklisted die or when new nodes join the network.

III. PROPOSED SYSTEM

A. System Overview

This approach facilitates trust decision making based on a lightweight scheme. This model can greatly improve system efficiency while reducing the effect of malicious nodes. By adopting a dependability enhanced trust evaluating approach for co-operations between CHs, LDTS can effectively detect and prevent malicious, selfish, and faulty CHs. Due to cancelling feedback between cluster members (CMs) or between cluster heads (CHs), this approach can significantly improve system efficiency while reducing the effect of malicious nodes .This model demands less memory and communication overhead as compared with other typical trust systems and is more suitable for clustered WSNs.

Trust Decision-Making at CM Level:

A CM calculates the trust value of its neighbours based on two information sources

1. Direct trust degree (DTD)
2. Indirect trust degree (ITD)

DTD is evaluated by the number of successful and unsuccessful interactions. In this work, interaction refers to the cooperation of two CMs. All CMs communicate via a shared bidirectional wireless channel and operate in the promiscuous mode, that is, if node sends a message to CH via node, then node can hear whether node forwarded such message to CH, the destination.

Trust Decision-Making at CH Level:

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

1. CH-to-CH direct trust and
2. BS-to-CH feedback trust.

During CH-to-CH communication, the CH maintains the records of past interactions of another CH in the same manner as CMs keep interaction records of their neighbours. Thus, the direct trust value can be computed according to the number of successful and unsuccessful interactions. The BS periodically asks all CHs for their trust ratings on their neighbours. After obtaining the ratings from CHs, the BS will aggregate them to form an effective value of ITD.

Formation of data collection node

DCN is set of data collection node. In DCT data, gather the information from its CH and then forwards the aggregated data packet to the destination node.

Intra Cluster Communication

Considering ambiguous expansive scale WSNs, sensor nodes have been densely deployed over the region. At the set-up stage, the beacon signal is utilized to distinguish the sensor nodes area and position. Once the nearby nodes are recognized, CH calculation is utilized to choose the CH.

DCT Communication

The DCT communication stage begins with intra cluster correspondence stage. In an intra-cluster correspondence process, a sensor node chooses itself as a CH to frame a cluster, at that point the CH is dependable to gather the information from its cluster members and cluster maintenance operations. From that point, tree arrangement is started, which associates the CH and sink. Presently, the sink starts the DCT development process. On the basis of CH and connection time, a few nodes are chosen as DCN (Data Collection Node) to create DCT.

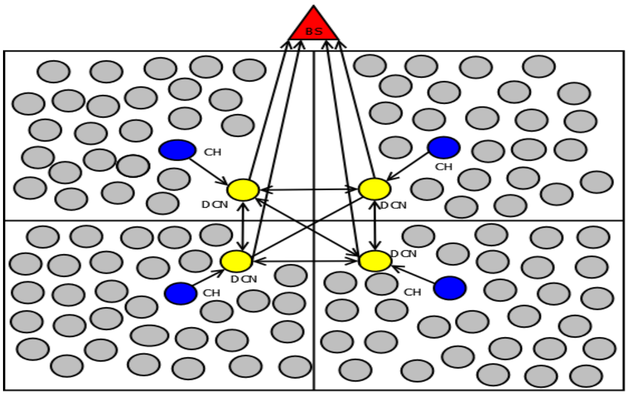

Figure 1. System Architecture

B. Algorithm Used

EECH is the dynamic clustering algorithm which uses an energy based threshold calculation to determine the cluster heads in the network. It uses multihop transmission from CH to BS to reduce energy consumption in network.

The probability of node being chosen as CH is based on Energy is given by:

Th(i) = $\frac{E(i)}{NE(c)}k$

Where, Th(i) – threshold of node i

k-average clusters in the network

E(i)- number of nodes in the network

E(c) – average energy in cluster c.

E(c) = $\frac{\sum E(i)}{N(c)}$

Where

$\sum E(i)$- summation of energy

N(c) – total nu of nodes in the clusters

The EECH algorithm uses multi-hop routing to transmit data from CH to BS, CH calculates its weight.

W(i) = $\frac{E(i)}{D_{to}BS(i)}$

Where,

W(i) = weight of node i

E(i) = Energy of node i

$D_{to}BS(i)$= Distance of node i from BS

If Wa < Wb < Wc then data goes to A→B→C→BS

C. Mathematical Model

This Let T be a system which shows as, T = {Input, Process, Output}

Input:

Sensing Information

M = {M1, M2, ….., Mn}

M is a set of input represents data i.e. Sensing information needs tobe sending to sink (Base Station).

Process:

1. Set of sensor nodes.

   N = {N1, N2, …., Nm}

   S = set of sensor nodes in a network.

   Set up phase

2. Cluster Formation by using ECH algorithm:-

   F = {F1, F2, ….,Fn}

   F is set of clusters created in setup phase.

   Each cluster contains a number of sensor nodes (F).

3. Cluster Head Selection

   For each Cluster Member calculates threshold value:

$$T = Flag + \frac{E * C}{D * S} + CM_{size}(1)$$

Where, T = Threshold

E = Energy of node

C = Coverage Range

D = Distance of node from the sink (Base Station).

S = Speed of node

CM_{size} = Size of cluster

Flag =$\begin{cases} 1, if\ node = cluster\ head \\ 0, \quad\quad\quad\quad otherwise \end{cases}$

T is the threshold of all nodes,
$Th=\{Th_{N1}, Th_{N2}, \ldots, Th_{Nn}\}$

Select CH as:
$CH_{Fn} = MIN(Th_{N1}, Th_{N2}, \ldots, Th_{Nn})$
Cluster head of all n number of clusters:

$CH_{Fn} = \{CH_{F1}, CH_{F2}, \ldots, CH_{Fn}\}$

4. Intra cluster Communication
Selection of Cluster head
CH = {CH1, CH2, …..,CHn}
CH is set of cluster heads, which are use full for communication among clusters.
For Cluster Fn,
Send Data as:

$$N_n \in F_n \xrightarrow{SendData(M=\{M1, M2, \ldots, Mn\})} CH_{Fn}$$

5. DCT Communication
Using equation 1, compute the threshold of all nodes, and select the node with lowest threshold as DCN. This node should not be assigned as CH previously.

$$CH_{Fn} \xrightarrow{SendData} DCN_{Fn}$$

In such a way that,

$DCN_{Fn} = MIN(Th_{N1}, Th_{N2}, \ldots, Th_{Nn})$,
$DCN_{Fn} != CH_{Fn}$

6. Data Recovery
A = Represent the data recovery process.
If the attack is found in DCN then Sink recovers data fromnearest data collection node (DCN).

Output: The authenticated aggregated data at Base Station securely.

$$DCN_n \in F_n \xrightarrow{SendData(M=\{M1, M2, \ldots, Mn\})} BS$$

Where, BS= Base Station.

IV. RESULT AND DISCUSSION

The performance of system is tested with the different sized network. The system is tested with 5 different networks consisting of 40, 50, 60, 70 and 80 nodes respectively.

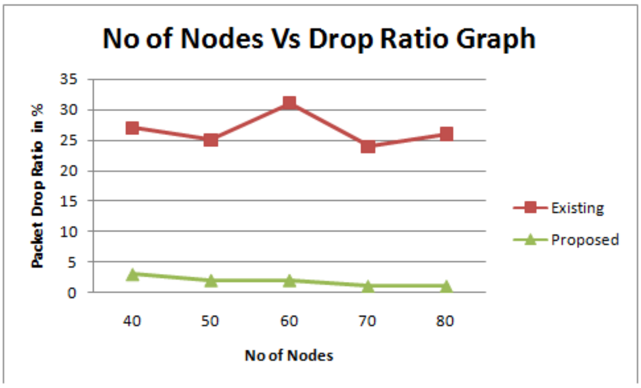

Figure 2. Packet Drop Ratio Comparison Graph

Figure 1 represent the graphical comparison of Packet Drop Ratio in existing and proposed the system with 5 different set of nodes or for different size of network respectively. X-axis represents the network with different size and Y-axis represents the Packet Drop Ratio in percentage. As data is verified at CH and DCN, packet drop becomes minimum in proposed System.

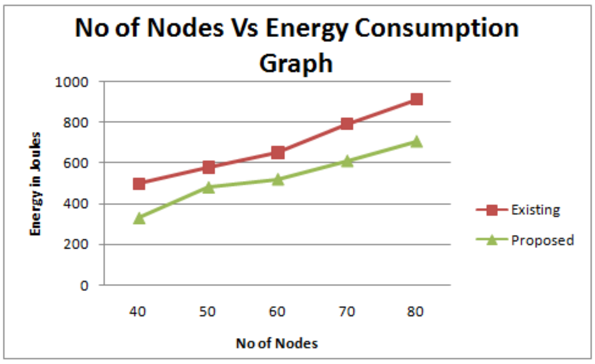

Figure 3. Energy Consumption Graph

Figure 3 represent the graphical comparison of energy consumption in existing and proposed the system with 5 different set of nodes or for different size of network respectively. X-axis represents the systems and Y-axis represents the energy consumed in Joules

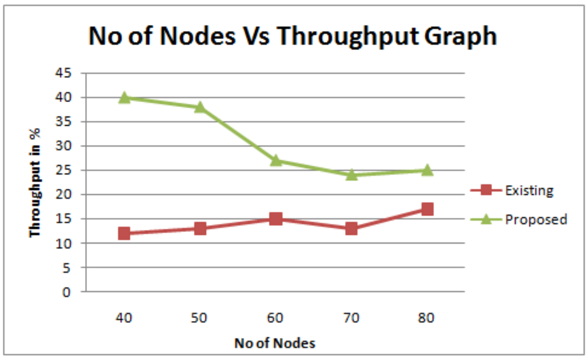

Figure 4. Throughput in %

Figure 4 depicts the comparison of the system based on throughput. Throughput is measured in terms of %. Throughput is the maximum rate of data packets reached to Base Station.

Figure 5 shows that the proposed system takes minimum time to forward the data from source to destination node that the existing system.

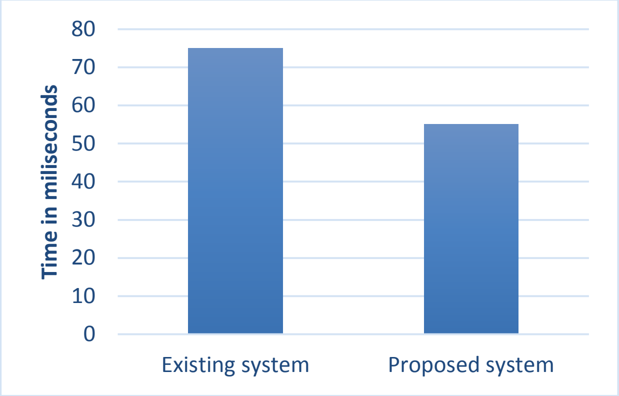

Figure 5. Time Graph Comparison

V. CONCLUSION AND FUTURE SCOPE

This framework can greatly improve system efficiency while reducing the effect of malicious nodes. By adopting a dependability-enhanced trust evaluating approach for cooperations between CHs, LDTS can effectively detect and prevent malicious, selfish, and faulty CHs. Due to cancelling feedback between cluster members (CMs) or between cluster heads(CHs), this approach can significantly improve system efficiency while reducing the effect of malicious nodes. cluster tree based mesh topology identify and prohibit the attacks on the cluster member, cluster head and data collection node(DCN). This makes the system protected. While every cluster member selects the cluster head and DCN on the basis of energy, distance, size, coverage range and size of the cluster. This enhances the efficiency of the network. Use of mesh topology in cluster tree does not permit malicious data to reach to the sinknode. This minimizes wastage of energy by denying malicious data and extends the network lifetime.

V. REFERENCES

1. FenyeBao, Ray Chen, MoonJeong Chang, and Jin-Hee Cho. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE transactions on network and service management, 9(2):169-183, 2012.
2. Garth V Crosby, NikiPissinou, and James Gadze. A framework for trust-based cluster head election in wireless sensor networks. In Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems, pages 10-pp. IEEE, 2006.
3. SaurabhGaneriwal, Laura K Balzano, and Mani B Srivastava. Reputation-based framework for high integrity sensor networks. ACM Transactions on Sensor Networks(TOSN), 4(3):15, 2008.
4. AblolfazlAfsharzadehKazerooni, HamedJelodar, and JavadAramideh. Leach and heed clustering algorithms in wireless sensor networks: a qualitative study. Advancesin Science and Technology Research Journal, 9(25), 2015.
5. Xiaoyong Li, Feng Zhou, and Junping Du. Ldts: a lightweight and dependable trust system for clustered wireless sensor networks. IEEE transactions on information forensics and security, 8(6):924-935, 2013.
6. Xiaoyong Li, Feng Zhou, and Xudong Yang. A multi-dimensional trust evaluation model for large-scale p2p computing. Journal of Parallel and Distributed Computing, 71(6):837-847, 2011.
7. Zhengqiang Liang and Weisong Shi. Trecon: A trust-based economic framework for efficient

internet routing. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 40(1):52-67, 2010. 15

8. Jaydip Sen. A survey on reputation and trust-based systems for wireless communication networks. arXiv preprint arXiv:1012.2529, 2010.
9. Riaz Ahmed Shaikh, Hassan Jameel, Brian J d'Auriol, Heejo Lee, SungyoungLee, and Young-Jae Song. Group-based trust management scheme for clustered wireless sensor networks. IEEE transactions on parallel and distributed systems, 20(11):1698-1712, 2009.
10. Ivan Stojmenovic. Handbook of wireless networks and mobile computing, volume 27. John Wiley & Sons, 2003.
11. Yan Sun, Zhu Han, and KJ Ray Liu. Defence of trust management vulnerabilities in distributed networks. IEEE Communications Magazine, 46(2):112-119, 2008.
12. Yan Lindsay Sun, Wei Yu, Zhu Han, and KJ Ray Liu. Information theoretic framework of trust modeling and evaluation for ad hoc networks. IEEE Journal on Selected Areas in Communications, 24(2):305-317, 2006
13. Dali Wei, YichaoJin, SerdarVural, Klaus Moessner, and Rahim Tafazolli. An energy-efficient clustering solution for wireless sensor networks. IEEE transactions on wireless communications, 10(11):3973-3983, 2011.
14. GuoxingZhan,Weisong Shi, and Julia Deng. Tarf: A trust-aware routing framework for wireless sensor networks. In European Conference on Wireless Sensor Networks, pages 65-80. Springer, 2010