DATA TRAFFIC TRUST MODEL FOR CLUSTERED WIRELESS SENSOR NETWORK

Dr. Senthilkumar A[1], Dr. Lekashri S[2], Abhay Chaturvedi[3], Dr.R.Manikandan[4]

[1]Assistant Professor, Kings Engineering College, Sriperumbudur , Chennai, India
senthilkumar@kingsedu.ac.in
[2]Associate Professor, Kings Engineering College, Sriperumbudur, Chennai, India
lekashri@kingsedu.ac.in
[3]Associate Professor, Department of ECE, GLA University, Mathura , U.P. , India
abhaychat@gmail.com
Co-Ordinator & Head, Department of CS, The Quaide Milleth College for Men
Chennai, India
manisankar27@gmail.com

Abstract: *Trust is an essential parameter among sensor nodes to provide secured and successful communication. Many trust management schemes have been proposed earlier for large scale Wireless Sensor Network (WSN) however not cooperates well in terms of low dependability, memory overheads, large communication etc, therefore a system called Data Traffic Trust Scheme (DTTS) for clustered WSN is proposed here. Here the trust nodes are identified through the data traffic sampling rate. The trust rate is identified through the number of sent and receive data packets and the malicious packets are diagnosed through the un-matching packet rate. The simulation results are evaluated to show the efficiency for the proposed scheme.*

Keywords: Data traffic, Trust evaluation, Clustering, Random Traffic Sampling, WSN.

1. Introduction

WSNs are generally a self organised network consists of a collection of tiny, low cost resource constriction Sensor Node's (SN's) usually designed to deploy in the hostile area for monitoring the events as well as to report the observed data in a continuous as well as discrete data [1]. The clustering techniques are generally applied to prolong the lifetime of the network in WSN [2]. WSN is usually operated in a high dynamic system topology i.e. the sensor nodes can be joined or leave the network at anytime and anywhere according to the locations. Due to the WSN deployment nature the SN's are easily susceptible to several kind of attacks such as on-off attack, man in the middle attack, Sybil attacks, etc., and it is less reliable, easily prone to network failures [3–5].

The nodes can be compromised by rival force that misguides the other presented normal nodes to misbehave by providing negative feedbacks, false positive messages, etc. Consequently, erroneous data forwarding among nodes originated due to false nodes will collapse the whole network. Whenever the SN itself becomes a malicious node because of resource constraints, trust establishment [6], cryptographic and authentication methods can be applied to prevent from such attack. Trust estimation methods are generally applied for the estimations of reliability, dependability and trustworthiness of nodes by determining their behaviours and protect them from malignant attacks for node survival [7].

2. Related Works

Several methods and approaches are proposed earlier to design the trusted network such as probability, fuzzy, weighted, Bayesian, game theory, neural network, entropy-based and miscellaneous trust computation methods [8]. These trust models are generally categorized into two subcategories namely node and data trust models. A Lightweight and Dependable Trust System (LDTS) for WSNs was proposed [9] that employs clustering algorithms to detect the node identities to verify the nodes. Node trust models are further divided into centralized and distributed trust model [10].

Binomial Distribution-based Trust Management Scheme (BDTMS) was proposed for healthcare-oriented WSN based on binomial distribution with high accuracy for resolving vulnerable security attacks [11]. BDTMS can effectively diagnose the on-off attack rapidly and effectively and therefore this scheme is considered to be safe and secure but increases computational cost. Bayesian-based trust management scheme was proposed for WSNs to detect and alleviate false nodes [12]. Two factors such as reward and penalty are used to determine trust among nodes along with attenuation function to update the

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

determined trust values.

Each nodes present in the cluster can communicate directly Cluster Head (CH) to reduce overheads leads in case of larger WSNs because the member of the cluster send their own trust values through the other cluster nodes which takes the particular trusted shortest path [13]. Trust based framework called Lightweight Trust-estimation Scheme (LTS) [14] was proposed that can be operated using a distributed approach such as intra-cluster and inter-cluster along respectively. This helps in finding accurate trust values of sensor nodes with minimum overheads. Here each and every sensor node calculate its neighbors' trust value on basis of a defined threshold value.

3. Proposed Method

In a hierarchical WSN sensing data and data relaying are the two major functions performed by the nodes. Sensor nodes or cluster members collect the information from the deployed region and transmit the same to their corresponding cluster head directly in single-hop or through multiple-hops path. SN's are grouped in to clusters and each CH is selected with the potential energy value of the node. CH has the ability to control the other nodes present in the group and transmits the data sensed by the nodes present in their group. A CH receives the data traffic from their presented sensor nodes and computes the trust values on the basis of random traffic sampling. Finally CHs delivers the trusted information to the BS.

The packets sent from one node to other should be a trusted one. The malicious nodes insert the malicious packets while routing the packets among various number of nodes towards the BS. Therefore the CH checks the traffic that received from the other nodes presented in the group. The trustworthiness of the data traffic is determined by random sampling method. If one of the packet among received is identified as malicious then the probability of the upcoming packets that are received in sequence with the malicious packet is considered to be malicious. The attacks can be performed in different ways like inserting malicious bits in one packet or inserting more number of malicious packets in the data traffic. Therefore the trust values is computed by assuming N number of packets sent from one node and I number of packets are proved to be trusted packets. Probability distribution of observing n(N)=n(I) is governed by using equation 1.

$$n(N) = n(\mathrm{I}) - \mathrm{n}(\mathrm{I}-\mathrm{k}) \qquad (1)$$

Here n(I-k) is denoted number of malicious packets included. The trust values for all the informations collected in CH is calculated through the number of normal data packets sent to the number of received data packets. If the number of sent packet traffic and the obtained packet traffic is equal (i.e. k=0) then the packets are noted as trusted packets and forwarded to the BS. Else if k receives some values (i.e. k=1, 2…n) then it is concluded that the data is included with malicious packets and it is dropped at the respective CH.

Each and every sender should record the number of packets that are sent by them. By taking an appropriate threshold, the malicious packets that are included during transmission can be recognized accordingly. This technique helps to decide whether the node is malicious on the basis of its data traffic set. The data_traffic threshold is set to identify the normal nodes and malicious nodes in order to remove the particular node from the routing system. The trusted traffic is verified in base of whether the traffic is received from the trusted nodes or not. The node has Trust value (Tval) and it is computed with its count of request and reply messages. If both request_sent and reply_received messages are equal then the node can be considered as normal node or trusted node. If both are not equal then it is tagged as malicious node and the traffic sent by the particular node is set as malicious traffic.

Random traffic sampling

Each node deployed in the system with signature-based trust component that can record each and every packet transmissions done by the particular node. Computation of trust is usually done on the basis of period of time 't' that consists of time cycles. The number of sensor nodes present in the cluster will record the traffic information which includes the total number of received and sent packets also the count of malicious packets that is received from other nodes present in the cluster in each unit of time and all the information are aggregated to its CH. The elapse time for traffic sampling includes the slides of time window to the right (one unit of time) and the nodes that drop the collected data for the purpose of minimizing the consumption of storage. Once the data received by the CH then the trust value is computed through the traffic sampling rate with respect to their threshold traffic rate. Finally the CH reports the results and sends data to the base station. Figure 1 shows the flow diagram of the proposed DTTS protocol.

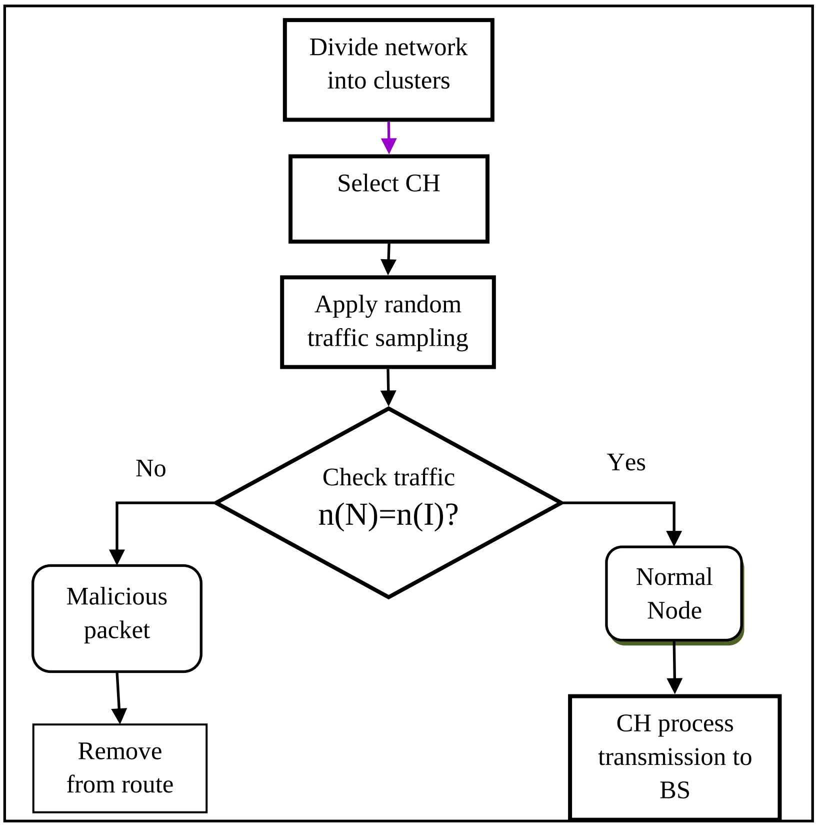
Divide network into clusters
Select CH
Apply random traffic sampling
Check traffic n(N)=n(I)?
No
Yes
Malicious packet
Normal Node
Remove from route
CH process transmission to BS

Figure 1: Flow diagram of DTTS

4. Results and Discussions

Network Simulator tool of version 2.35 is used here for simulating the proposed DTTS method and existing LTS protocol. NS2 has its own advantages and validating with this tool makes the protocols more computational efficient. It has simple scalability factor by using tool command language. The simulation area is taken here in the dimensions of 1000X800 meters deployed with 100 number of nodes.

The parameters taken for analyzing the proposed scheme are Data Rate Delivered (DRD), False Detection Rate and Energy Consumption.

Data Rate Delivered

Data rate that is delivered to the sink node is determined by taking the difference of rate of transmitted data packets from sender to the rate of received data packets to receiver. It is computed using equation 2, here n represents number of nodes.

$$DRD = \frac{\sum_{o}^{n} PktRcv(n) - \sum_{o}^{n} PktSent(n)}{Time} \qquad (2)$$

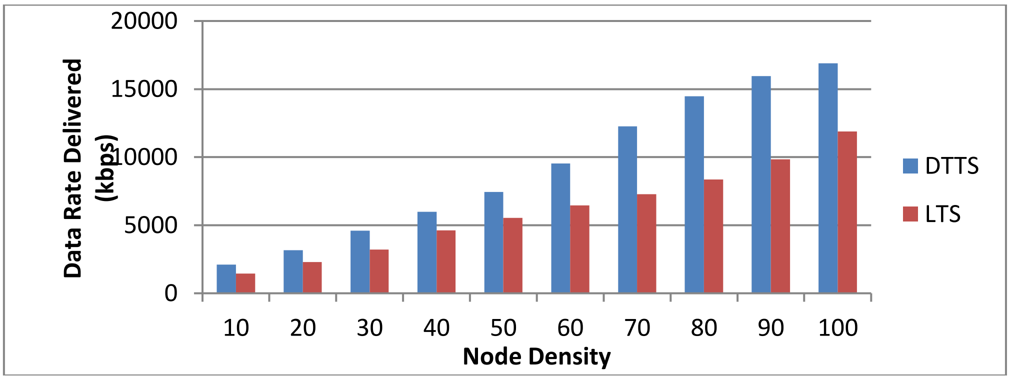

Figure 2: Data Rate Delivered

The data rate that delivered to the base station for the proposed DTTS and conventional LTS scheme is shown in figure 2. The DTTS scheme (our proposed model) achieves better delivery rates in terms when compared with LTS method.

Node Trust Factor

The trust factor is estimated to identify the average number of trustable nodes that presented in the routing. To precisely check whether the node is malicious or not the data packets are sampled here with respect to the sent and received packet counts. The average trust ratio for the proposed method is 0.85 and for LTS the obtained average trust ratio is 0.78. Therefore the DTTS scheme has high detecting capability since it has high node trustability factor.

Figure 3 shows that node trust factor for both DTTS and LTS schemes and DTTS proved to be better in terms of trustable factor.

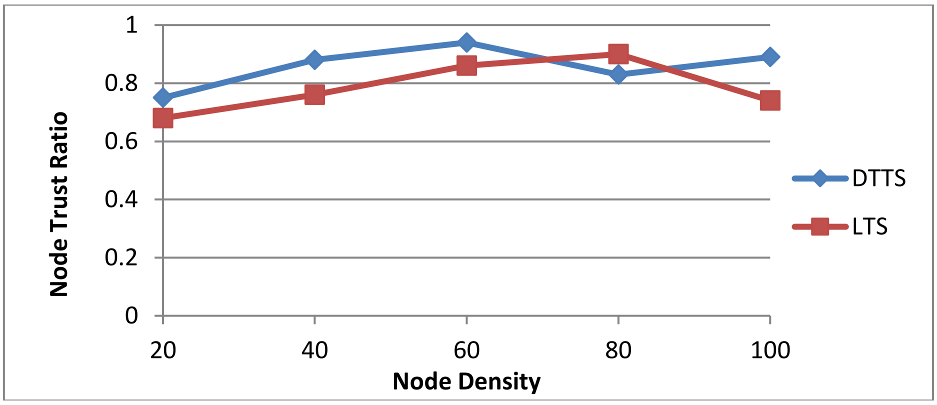

Figure 3: Node Trust Factor

Energy Leftover

The energy level that is left for further transmission after the completion of certain level of data processing and transmissions from one node to other is said to be residual or energy leftover. The node's energy level is mostly utilized for sensing, transmitting and receiving the information.

The energy leftover that is obtained for both proposed DTTS and conventional LTS scheme is shown in figure 4, the proposed protocol consumes less energy when compared with conventional protocol since the data's are processed through CH.

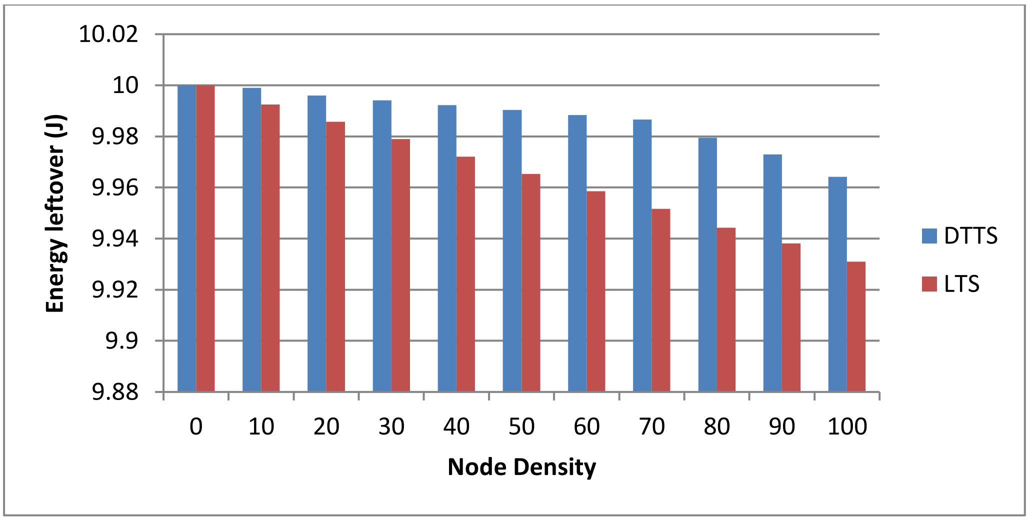

Figure 4: Energy Consumption

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

5. Conclusion

Data Traffic Trust Model for clustered WSN is proposed here. A CH receives the data traffic from their presented sensor nodes and computes the trust values on the basis of random traffic sampling. Here the trust nodes are identified through the data traffic sampling rate. The trust rate is identified through the number of sent and receive data packets and the malicious packets are diagnosed through the un-matching packet rate. CH is selected on basis of high potential energy that is left in the nodes. Finally CH delivers the trusted information to the BS. Simulation results are shown that the efficiency of the proposed scheme is better in terms of delivery rate, energy leftover and trust factor.

References

1. Ganesh, S., & Amutha, R. (2012). Efficient and secure routing protocol for wireless sensor networks through optimal power control and optimal handoff-based recovery mechanism. *Journal of Computer Networks and Communications*, *2012*.

2. Thangaraj, K., & Selvi, T. (2015). Efficient and Secure Routing Protocol for Wireless Sensor Networks through SNR Based Dynamic Clustering Mechanisms. *i-Manager's Journal on Wireless Communication Networks*, *3*(4), 14.

3. Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H. C. (2014). Management and applications of trust in Wireless Sensor Networks: A survey. *Journal of Computer and System Sciences*, *80*(3), 602-617.

4. Feng, R., Xu, X., Zhou, X., & Wan, J. (2011). A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory. *Sensors*, *11*(2), 1345-1360.

5. Mohammadi, S., Atani, R. E., & Jadidoleslamy, H. (2011). A comparison of routing attacks on wireless sensor networks. *organization*, *4*, 21.

6. Ishmanov, F., Kim, S. W., & Nam, S. Y. (2014). A secure trust establishment scheme for wireless sensor networks. *Sensors*, *14*(1), 1877-1897.

7. Talbi, S., Koudil, M., Bouabdallah, A., & Benatchba, K. (2017). Adaptive and dual data-communication trust scheme for clustered wireless sensor networks. *Telecommunication Systems*, *65*(4), 605-619.

8. Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K., & Khan, A. W. (2015). A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks. *Frontiers of Computer Science*, *9*(2), 280-296.

9. Li, X., Zhou, F., & Du, J. (2013). LDTS: A lightweight and dependable trust system for clustered wireless sensor networks. *IEEE transactions on information forensics and security*, *8*(6), 924-935.

10. Karthik, N., & Ananthanarayana, V. S. (2017). A hybrid trust management scheme for wireless sensor networks. *Wireless Personal Communications*, *97*(4), 5137-5170.

11. Fang, W., Zhu, C., Chen, W., Zhang, W., & Rodrigues, J. J. (2018, June). BDTMS: Binomial distribution-based trust management scheme for healthcare-oriented Wireless Sensor Network. In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 382-387). IEEE.

12. Zhang, M. (2017, October). Trust computation model based on improved Bayesian for wireless sensor networks. In *2017 IEEE 17th International Conference on Communication Technology (ICCT)* (pp. 960-964). IEEE.

13. Ambreen, N. H. (2013). Wireless sensor network through shortest path route. *International Journal of Emerging Technology and Advanced Engineering*, *3*(2), 158-161.

14. Khan, T., Singh, K., Abdel-Basset, M., Long, H. V., Singh, S. P., & Manjul, M. (2019). A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks. *IEEE Access*, *7*, 58221-58240.

15. Manikandan, R., Latha, R., & Ambethraj, C. (1). An Analysis of Map Matching Algorithm for Recent Intelligent Transport System. Asian Journal of Applied Sciences, 5(1). Retrieved from https://www.ajouronline.com/index.php/AJAS/article/view/4642.

16. R. Sathish, R. Manikandan, S. Silvia Priscila, B. V. Sara and R. Mahaveerakannan, "A Report on the Impact of Information Technology and Social Media on Covid–19," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 224-230, doi: 10.1109/ICISS49785.2020.9316046.