Volume 3, Issue 9, September 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security Enhancement Based on Trust Aware Routing in Wireless Sensor Networks

Suneyna
M.Tech Student
ECE Deptt. , Vaish College of Engineering, Rohtak, India

Bhavneesh Malik
Assistant Professor
ECE Deptt. , Vaish College of Engineering, Rohtak, India

Abstract- Wireless Sensor Networks (WSNs) offer solutions which cover a wide range of application domains, including homeland security and personal healthcare, building and urban surveillance, industrial operations and environmental monitoring. The sensor nodes are dynamic in their behavior; hence routing is upgraded at different instants of time. Two parameters are considered in routing, while dividing the sensor nodes into different clusters and ensured with trust and weight of each node to be in the path of routing. In this research, consideration is on one parameter that is trust value. Each node has direct and indirect trust values assigned, which are used for security check of the node. A trust based algorithm will be proposed for detecting suspicious transmission and consequent identification of malicious nodes for disseminating this information in the network and a comparison will be done with existing approaches regarding packet loss, packet delivery ratio, latency and throughput through simulation results.

Keywords- Clustering, WSN, Trust, Weight, Security.

I. INTRODUCTION

In wireless and mobile computing the major challenging design factor is the issue of secure routing in different networking aspects. The nature of WSN complicates the security requirements and adds difficulties in solving security problems [1]. One of the most special aspects in WSN is the provision of secure routing. In fact, secure routing in WSN is actually still not captured well in the research field. One main reason is that the design of a routing protocol is biased towards solving the problem of power limitations and reducing communication overhead and while keeping security concerns in a later phase to be integrated with the current routing solutions [2]. Ensuring routing security is a necessary requirement to guarantee the success of routing operation. When we talk about secure routing, we are concerned with security problems that may occur due to improper actions from an assumed router [3].

II. TRUST AWARE ROUTING [5]

Trust is an old but important issue in any networked environment, whether social networking or computer networking. Trust can solve some problems beyond the power of the traditional cryptographic security. Trust management is the key to build trusted, dependable wireless sensor network applications. The trust issue is emerging as sensor networks thrive. However, it is not easy to build a good trust model within a sensor network with limited resources. Furthermore, in order to keep the sensor nodes independent, we should not assume there is a trust among sensors in advance. A trust aware routing protocol is a routing protocol in which a node incorporates in the routing decision its opinion about the behavior of a candidate router. This opinion is quantified and called the trust metric. Trust metric should reflect how much a router is expected to behave, for example, forward a packet when it receives it from a previous node [7]. Obtaining the trust metric is a problem by itself since it requires several operational tasks on observing nodes behavior, exchanging nodes' experience and opinions as well as modeling the acquired observations and exchanged knowledge to reflect nodes trust values. A system that provides these tasks to ultimately output a "rating" or a trust value on nodes is called a reputation system.

III. REQUIREMENT OF TRUST AWARE ROUTING

Trust aware routing [4] in WSN is important for both securing obtained information as well as protecting the network performance from degradation and network resources from unreasonable consumption. Most WSN applications carry and deliver very critical and secret information like in military and health applications. WSN's infected by misbehaving nodes can misroute packets to wrong destinations leading to misinformation or do not forward packets to their destination leading to loss of information. Such critical applications can be very sensitive to these attacks. Having a trust aware routing protocol [9] can protect data exchange, secure information deliver and protect the value of communicated information. Node misbehavior can cause performance degradation as well. An infected open WSN can be partitioned into different parts that cannot communicate among each other due to non forwarding attacks. This leads to the demand of increasing the number of sensors or changing the node deployment to return network connectivity. But it is very expensive, however, can be avoided if a good secure routing solution is adopted.

IV. PROPOSED WORK

One factor which is trust value; is taken into consideration. At first, malicious node is detected and clusters are made leaving the malicious node. Then CH is chosen on the basis of trust value for all clusters. CH having the best trust value is chosen as secured path for data transmission. Following steps are taken into account to achieve the goal:

1. Initially take 40 nodes.
2. Detect malicious nodes on the basis of threshold energy [8] using following equation:

   $W_n = w_n - \Theta \times R_n$

   Where

   R_n = m/s or malicious nodes/ total nodes
3. Remove malicious nodes and make clusters of rest of the nodes by using the following equation of aggregation result:

$$AR = \sum_{i=0}^{n} W_n . U_n$$

Where AR = Aggregation Result

W_n = Weight of each node (0 to 1)

U_n = Output of each sensor node (0 or 1 for digital communication)

n = Number of nodes in a cluster

4. CH is chosen on the basis of trust values assigned to each node by using equation :

$$T_r(u) = i = \sum_{i=0}^{n} \frac{T_u \times T_d}{T_d}$$

And Trust sudation will be done using equation-

$$T(u) = \propto \times T_d(u) + \beta T_r(u)$$

Where

T (u) ⟶ Trust value of node u and 0 < T <=10.

T_r (u) ⟶ Indirect trust value of node u

T_d ⟶ Trust value of node i

5. Transmission takes place on the basis of CH having the best i.e. largest trust value.

V. RESULTS

As random nodes are deployed in the environment. Malicious node is detected on the basis of threshold energy. After the detection and removal of malicious node clusters are made and CH are made among all clusters. After that CH's are assigned with calculated trust value. CH having largest trust value is taken as transmission path which also shows increment in generated and received packets and reduction in loss rate and latency. Results are taken for both existing and proposed work for 3 clusters and 4 clusters. In the existing work, CH are chosen on the basis of threshold value while in proposed work, CH are chosen on the basis of trust value.

Parameters

Packet Delivery Ratio(PDR): It is defined as the ratio of packet delivered at the destination to the packet send.

Latency: It is the time taken by the packet to reach at destination. It can also be defined as end to end delay.

Throughput: It is the average rate of successful packet delivered to the destination.

TABLE 1: PERFORMANCE ANALYSIS OF EXISTING AND PROPOSED SYSTEM ON THE BASIS OF VARIOUS PARAMETERS FOR 3 CLUSTERS

Clusters	Generated Packets	Received Packets	Packet Delivery Ratio (PDR)	Loss Rate	Latency
3 Clusters Existing	21668	21344	98.5047	0.0119993	258.74
3 Clusters Proposed	22406	22041	98.371	0.00830135	230.151

This table shows comparison among parameters generated packet, received packet, PDR, loss rate and latency for 3 clusters.

TABLE 2: PERFORMANCE ANALYSIS OF EXISTING AND PROPOSED SYSTEM ON THE BASIS OF VARIOUS PARAMETERS FOR 4 CLUSTERS

Clusters	Generated Packets	Received Packets	Packet Delivery Ratio (PDR)	Loss Rate	Latency
4 Clusters Existing	19907	19341	97.1568	0.0160245	287.899
4 Clusters Proposed	22273	21844	98.0739	0.0133345	268.5

This table shows comparison among parameters generated packet, received packet, PDR, loss rate and latency for 4 clusters.

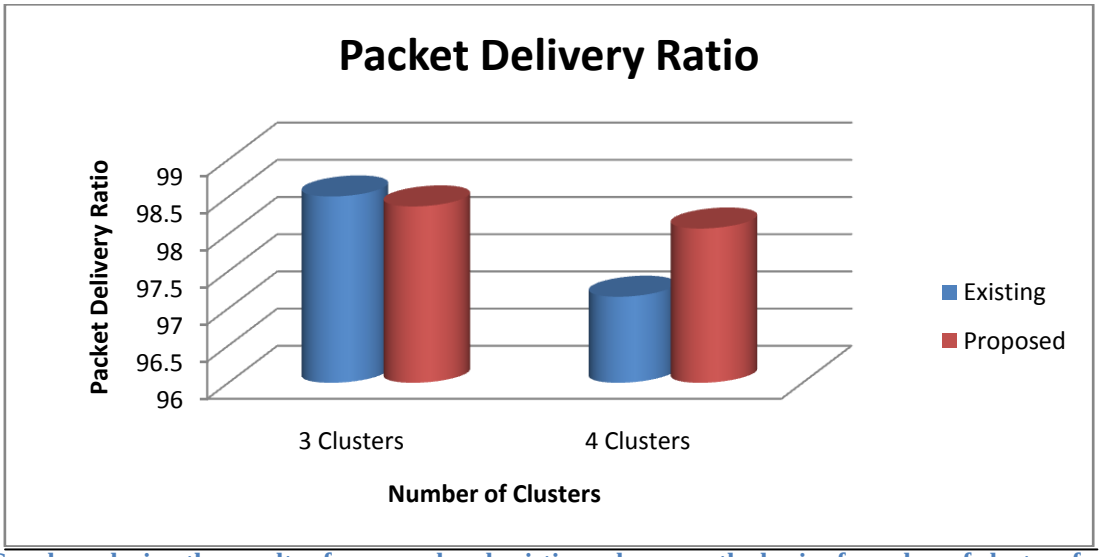

Fig. 1: Graph analyzing the results of proposed and existing scheme on the basis of number of clusters for Packet Delivery Ratio (PDR)

This graph depicts Packet Delivery Ratio for both existing and proposed work for 3 clusters and 4 clusters.

Fig. 2: Graph analyzing the results of proposed and existing scheme on the basis of number of clusters for Loss Rate

This graph depicts reduction in loss rate for both existing and proposed work for 3 clusters and 4 clusters.

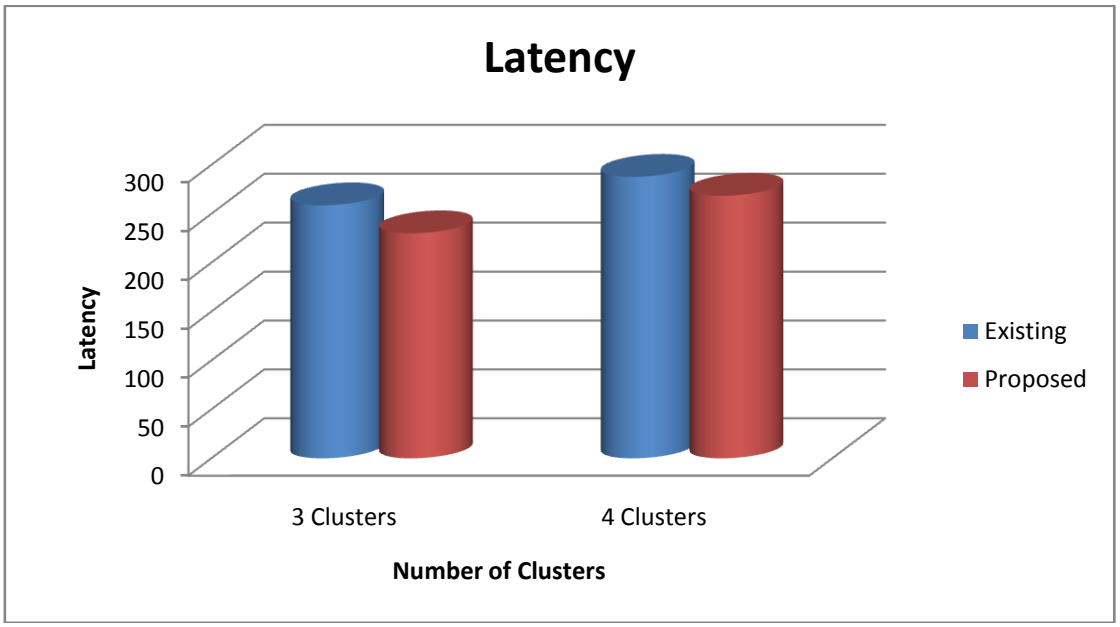

Fig. 3: Graph analyzing the results of proposed and existing scheme on the basis of number of clusters for Latency

This graph depicts reduction in latency for both existing and proposed work for 3 clusters and 4 clusters.

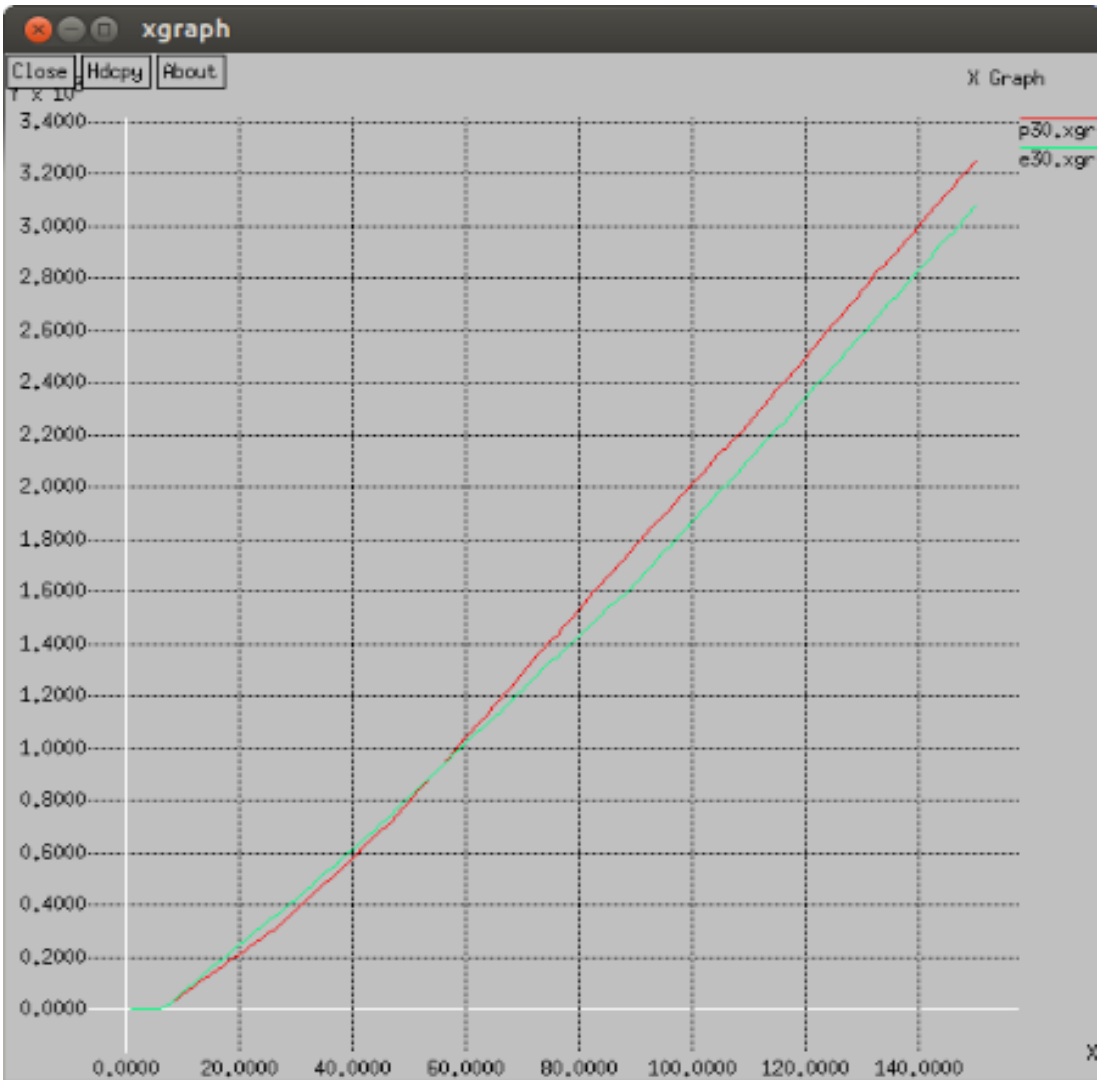

Fig. 4: Graph showing performance of existing and proposed scheme for 3 clusters

This graph depicts increment in throughput among existing and proposed work for 3 clusters.

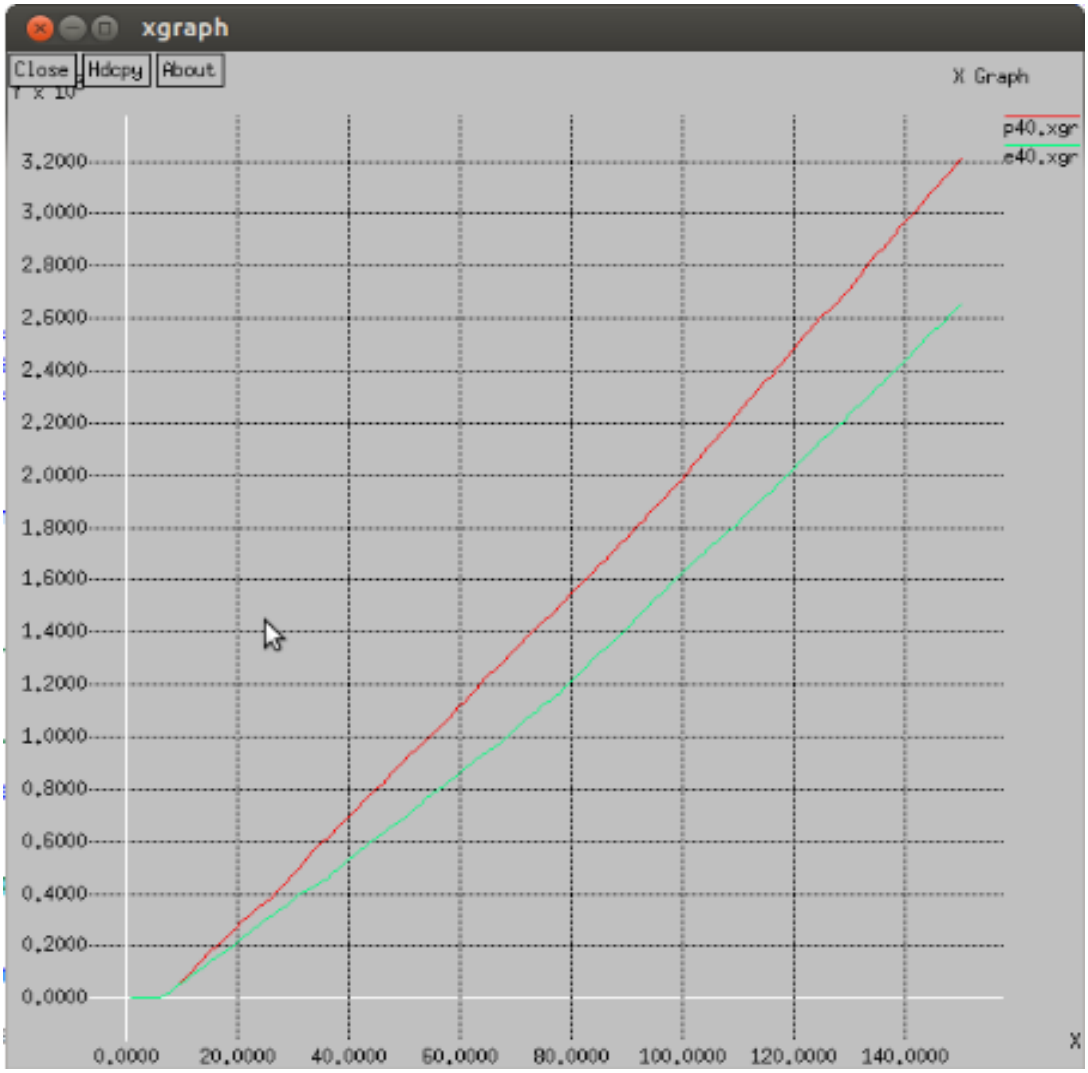

Fig. 5: Graph showing performance of existing and proposed scheme for 4 clusters

This graph depicts increment in throughput among existing and proposed work for 4 clusters.

VI. CONCLUSION

In this research, work is mainly done on the drawbacks of sensor network and security issues of WSN. The sensor nodes of network are dynamic in their behavior; hence routing is upgraded at different instants of time. Two parameters are considered in routing, while dividing the sensor nodes into different clusters and ensured with trust and weight of each node to be in the path of routing. Here we are considering only one parameter that is trust value. Each node has direct and indirect trust values assigned, which are used for security check of the node. A trust based algorithm is proposed for detecting suspicious transmission and consequent identification of malicious nodes for disseminating this information in the network. The simulation result shows that, there is lot of reduction in the packet loss, packet delivery ratio, latency and throughput when compared to the existing approach. Simulation is done in NS2 using the C++ coding, dynamism is provided to the network such that nodes are moving due to which nodes exhibit different trusts values with change in their path while routing.

REFRENCES

[1] Akyildiz, I.F., Melodia, T., and. Chowdhury, K., "*A survey on wireless multimedia sensor networks."* Computer Networks, vol.51, issue4: p. 921-960, 2007.

[2] A. Perrig, J. Stankovic, D.Wagner, "*Security in Wireless Sensor Networks"*, Communication of the ACM, June 2004.

[3] Adrian Perrig, John Stankovic, and David Wagner, "Security in wireless sensor networks" . Commun.ACM, 47(6):53{57, 2004.

[4] A. Pirzada, C. McDonald, "*Establishing Trust In Pure Ad-hoc Networks"*, Proceedings of the 27th conference on Australasian computer science, 2004.

[5] N. Noury, T. Herve, V. Rialle, G. Virone, E. Mercier, G. Morey, A. Moro, T. Porcheron,"Monitoring behavior in home using a smart fall sensor", IEEE-EMBS Special Topic Conference on Micro-technologies in Medicine and Biology, October 2000, pp. 607–610.

[6] K. Nagarathna, Kiran Y. B, J D. Mallapur, S. Hiremath (2012) worked on "Trust Based Secured Routing in Wireless Multimedia Sensor Networks", 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks.

[7] Theodore Zahariadis, Helen Leligou, Panagiotis Karkazis, Panagiotis Trakadas, Ioannis Papaefstathiou, Charalambos Vangelatos, Lionel Besson, "Design And Implementation Of A Trust-Aware Routing Protocol For Large Wsns", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010.

[8] Idris M.Atakli ,Hongking Hu, Yu Chan, " Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evalution ," The Symposis on Simulation of systems Security(SSSS 08),Ottawa,Canada, April 14 17,2008.

[9] Janani.C and Mrs. P.Chitra, "*Trust Evaluation Based Security In Wireless Sensor Network*", (IJITR) International Journal Of Innovative Technology And Research, Volume No. 1, Issue No. 1, December-January 2013, 054-060.

