Efficient Routing in Wireless Sensor Network using Fuzzy based Trust Model

Radhika A. Raje
Dept. of Computer Science
G. H. Raisoni College of Engineering
Nagpur, India

Apeksha V. Sakhare
Assistant Professor, Dept. of Computer Science
G. H. Raisoni College of Engineering
Nagpur, India

***Abstract*— Wireless sensor network consist of large number of sensor nodes that are deployed in large number to monitor the environment. In last few years there is a great technological advancement in wireless sensor network. Due to low-cost, small-size, nature of Wireless Sensor Networks (WSNs), it allows them to sense the information in various hostile environments (e.g. military surveillance, battlefield). So, to fully achieve the capacity of WSNs, sensor nodes need to cooperate in the collection and must disseminate topology information. These sensor nodes specifically operate in a multihop routing. In muiltihop routing, sensor network have to face a variety of risks due to the harsh operating environments. In this paper a fuzzy based approach is introduced which will enhance the routing security and reliability in WSNs.**

***Index Terms*—Wireless sensor network, Trust, Routing, Fuzzy Logic, Security.**

I. Introduction

Wireless sensor network are highly distributed network which consist of hundreds or thousands of small and lightweight wireless nodes. These nodes are connected via radio link and deployed in large number to monitor their surrounding environment or system. Each sensor node detects some events or collects information and communicates it in a wireless manner. Each of these scattered nodes has capability to route data to other sensor nodes or to base station [2].

Though there are technologies for networking and security, wireless sensor network still face some problem. As these networks operate in ad hoc manner, nodes are self organized. Due to self organized nature of sensor network malicious node may enter the network and eavesdropping can be easily performed. So, the communication here is multihop communication and is mainly relying on cooperation among nodes to achieve basic networking task like routing. In this each node sensed the data and forwards it to sink node which looks for available neighbor. So, this makes network to get exposed to privacy attack that ultimately disturb the network operation. As this network operate in multihop routing, is exposed to attacks identity deception through replaying routing information. Due to the identity deception, attacker may interfere with nodes and cause damage, drop or misdirect messages, create traffic collision or jam the communication channel. In a poor network connection distinguishing between an attacker and an honest node causes much difficulty. Obtaining a trusted relation among nodes is an important goal. WSNs which provide number of opportunities at same time it is exposed to dreadful challenges such as energy. So, it is important to consider energy use for sensor node at same time to consider security as one of the important goal.

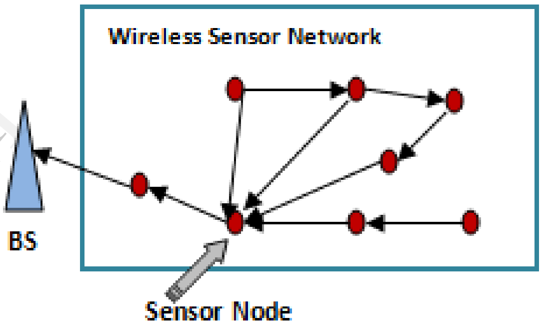


Fig.1. Multihop Communication in WSN

The paper is organized as follows: Section 2 reviews the existing work on WSN, its major attacks, prevention techniques and other existing movements to make WSN a promising network. Section 3 proposes the problem definition and objective of the paper. Section 4 introduces the new system; Section 5 illustrates the scenario which is considered. In section 6 simulation parameters are shown. Finally section 6 summarizes the overall work performed.

II. Related Work

A. TARF

This framework is developed for secure routing in wireless sensor network. In this[1] two parameters run on every sensor node to keep track of their trustworthiness and energy. As these parameter run on every sensor node it may increase the considerable overhead and it is developed on TinyOs.

B. FBSR

It utilizes feedback information in order to represent current states of neighbor nodes. This protocol consists of local independent forwarding decisions based on current feedback information and prediction of future conditions. FBSR [3] which uses a statistics-based detection on a base station to discover compromised nodes, is resilient against wormhole and Sybil attacks and is never evaluated or examined; FBSR use Keyed-OWHC-based authentication which causes considerable overhead.

C. TARP

It is a trust-based routing scheme responsible for routing messages from the different nodes to the base station. It is based on idea of node cooperation which forwards the neighbor messages. It uses the concept of cooperation in terms of routing reputation. TARP [4] achieves significant improvements in terms of energy consumption and scalability. This protocol exploits nodes' past routing behavior and link quality to determine efficient paths, but it does not offer protection against the identity deception through replaying routing information.

D. TAODV

All routing protocols in the ad hoc find the shortest path to the destination even if there is presence of any malicious node in that path, there is an internal threat in the network in the form of a compromised node. So a path free of malicious node is more important than the shortest path. This motivation force to design. TAODV [5]which is an extension of the AODV routing protocol. This protocol defined three procedures: trust recommendation, trust judgment , trust update. With this it also define route discovery and maintaining routing table.So in TAODV there is small increase in overhead with lesser speed because of the retransmission of some route request packets due to delayed receipt of route reply by the source nodes.

E. ATSR

It is a location-based trust-aware routing solution is introduced for large WSNs. ATSR [6] constitute a distributed trust model that utilizes both direct and indirect trust, authentication, geographical information in order to protect the WSNs from packet alteration, packet mis-forwarding, and acknowledgments spoofing. But this protocol does not offer protection against the identity deception.

F. SPIN

It is a data-centric routing where the nodes advertise the available data through an ADV and wait for request from interested node. Here it maintains two secure building blocks. First is a SNEP which protects the network from eavesdropping because it introduces small overhead of 8 bytes and it also maintains counter but no counter values are exchanged. Second is a µTesla which provides authentication to broadcasted data. SPIN [7] ensures data authentication and confidentiality claim by provide trusted routing. But it does not deal with compromised nodes or denial of service attacks, only it ensures that all the keys of the network node should not disclose by a compromised node.

III. PROBLEM DEFINITION AND OBJECTIVE

Existing routing protocol do not provide protection against identity deception, either assume honesty of nodes or attempt to exclude unauthorized participation by encrypting data and authenticating packets. The countermeasures proposed so far strongly depend on either tight time synchronization or known geographic information while their effectiveness against attacks exploiting the replay of routing information has not been examined yet. The objective is to introduce such approach which will exploit the replay of routing information against harmful attackers and overcome the problems like overhead, poor reliability, integrity in order to provide better security and efficient routing in WSN.

IV. PROPOSED WORK

To overcome problem of existing method, a fuzzy based trust model is introduced. In the following flow diagram proposed scheme is explained. FBTM enables a node to keep track of the trustworthiness of its neighbours and there by select a reliable route path. This trust Model based on Fuzzy Logic provide better security and survival of wireless sensor network under harsh and hostile environment.

Step 1: Initial sensor network.
Step 2: Run cluster election algorithm so the energy wastage can be avoided as sensor directly communicates to base station.

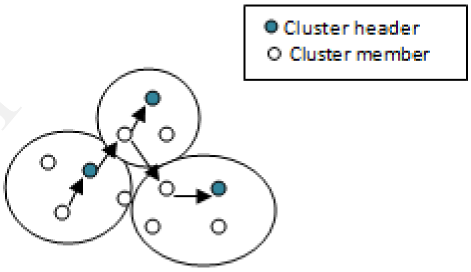


Fig.1.Cluster formation in wsn

Step3: Trust based clustering will be performed so the compromised or malicious node should not selected (elected) as a cluster head.
Step 4: Running trust monitor and energy supervisor parameter on cluster header only.
Step 5: Through this a nodes trust level and energy can be find out
Step 6: Then apply the fuzzy rules to cluster header to decide which node should be select as a next hop node to forward a data to base station.

The above steps are explained as follows:

To route a data packet to the base station, a node need to decide to which node it should forward a data packet. In initial sensor network after performing a cluster head election algorithm, the trust based clustering must be performed so the compromised node should not get selected as a cluster header. So here we assume each node has three keys; a master, cluster and pair wise. The master key is shared by every node and it facilitate broadcast by the base station. Members of each cluster share the cluster key. Each cluster has a different cluster key. This key facilitates multicasting communication from the base station to a cluster and also group communication within the clusters themselves. The pair wise key allows node-to node communication. After the parameter run on cluster header, in each cluster the cluster members are assigned 0.5 values as a trust value initially. A node's N trust monitor decides the trust level of each neighbor based on network loop discovery and broadcast from base station. Energy cost of its neighbor is defined as delivering data successfully from N to the base station with this neighbor as its next hope node .With the help of this cluster will be able to decide to which node it should forward a data to base station by applying fuzzy rules.

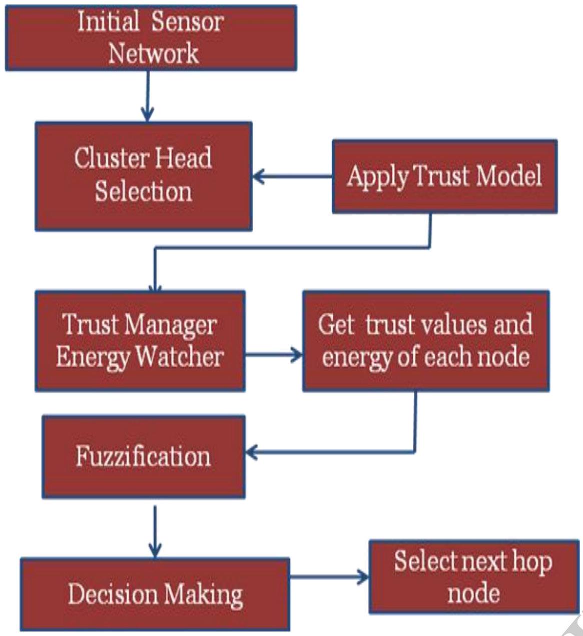


Fig.2.Flow diagram of proposed model

A. Energy Monitor

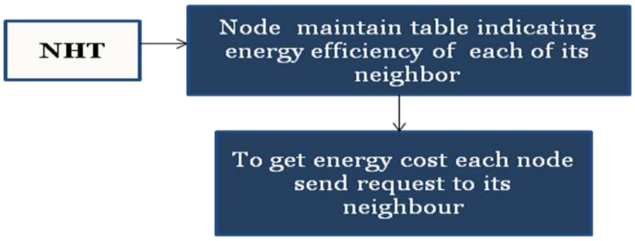

NHT
Node maintain table indicating energy efficiency of each of its neighbor
To get energy cost each node send request to its neighbour

Fig.3.Neighborhood table contain energy cost

B. Trust Tracer

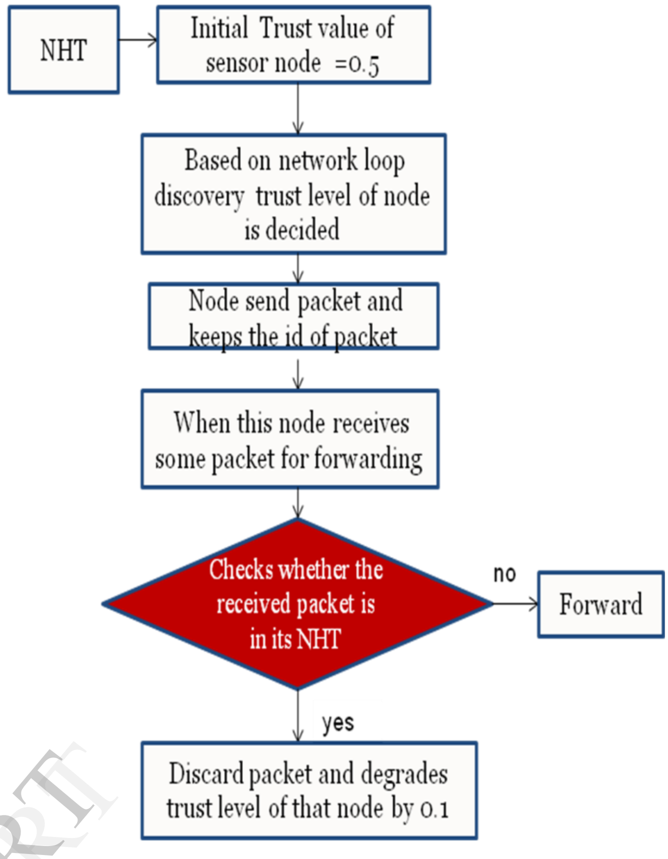

NHT
Initial Trust value of sensor node =0.5
Based on network loop discovery trust level of node is decided
Node send packet and keeps the id of packet
When this node receives some packet for forwarding
Checks whether the received packet is in its NHT
no
Forward
yes
Discard packet and degrades trust level of that node by 0.1

Fig.4.Flow diagram of trust tracer

C. Fuzzy Logic

Fuzzy logic is used when a node detects an event and wants to transmit packet .So; it selects an optimal neighbor within transmission range as its next hop and makes an decision. Using fuzzy logic technique, it is capable of selecting optimal routing path from the source node to the sink by favoring highest remaining energy and minimum number of hops.

The fuzzy logic used for decision making.
For these, fuzzy uses if-then rules which consider the following parameters.
Fuzzy Set = [{Trust, Distance, Energy}]
Decision is made on the basis of the output of the equivalent members of the fuzzy sets of these parameters.

TRUST	DISTANCE	ENERGY CONSUMED	RESULT
High	Low	Low	Best
High	Low	High	Normal
Low	High	Low	Normal
Low	High	Low	Worst
High	High	Low	Worst

TABLE I:FUZZY RULES

Above table shows the condition for the fuzzy logic in order to make a decision. According to the above table, after getting trust and energy value of node based on its performance the decision will be taken. Here some threshold value is decided for trust value. If obtained value is above the threshold then it is considered as high, if it is below that value then trust of that node is considered as a low. On the basis of result the decision will be taken .So , the result is in the form of best, normal and worst nodes. From this the best and normal nodes are considered for routing packet to the sink node.

V. SCENARIO

A. Sensor Network Communication Model

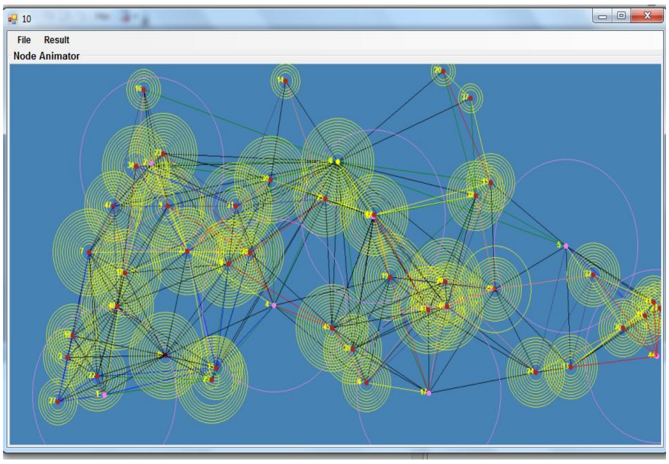


Fig.1. Sensor Network Communication

In the above scenario 50 nodes are considered and here yellow color shows nodes communication range.

B. Cluster Head Selection

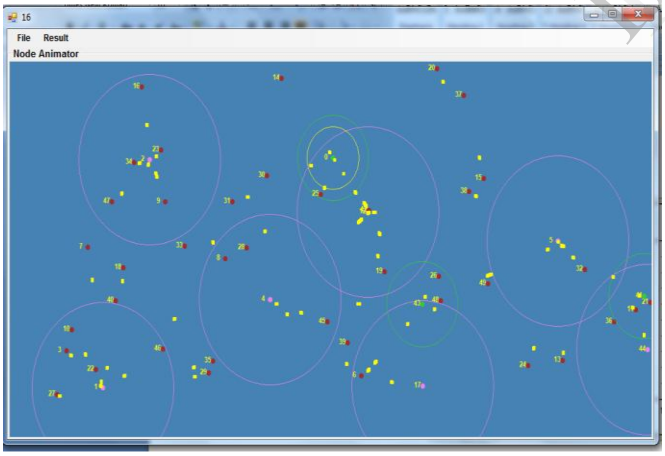


Fig.2. Clustering in WSn

In the above scenario 50 nodes are considered and trust based clustering is performed. The red nodes denoting sensor nodes and green nodes are misbehaving nodes and nodes with a range shows cluster header communication range.

VI. RESULTS

A. Energy

In the below snapshot the simulation analysis is shown. Here the graph is plot between simulation time of 14sec as a X-axis and Energy in joules as Y-axis. Energy is defined as average energy consumed for data transmission. So the energy efficiency for fuzzy based trust model shows better result.

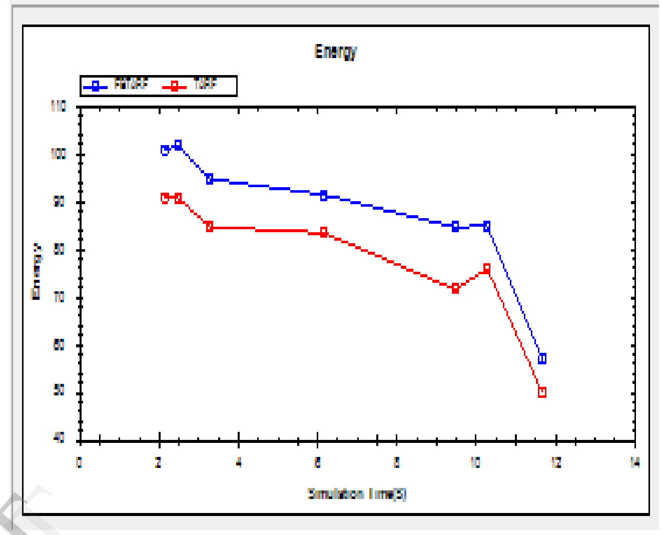


Fig.1. Performance Analysis: Energy

B. Packet delivery Ratio

Packet delivery Ratio is defined as a number of packets received successfully and the total number of packets transmitted. In the below snapshot the simulation analysis is shown. Here the graph is plot between simulation time of 14 sec as a X-axis and PDR in percentage as Y-axis. So here two protocol values are compared and PDR using fuzzy based routing shows better results.

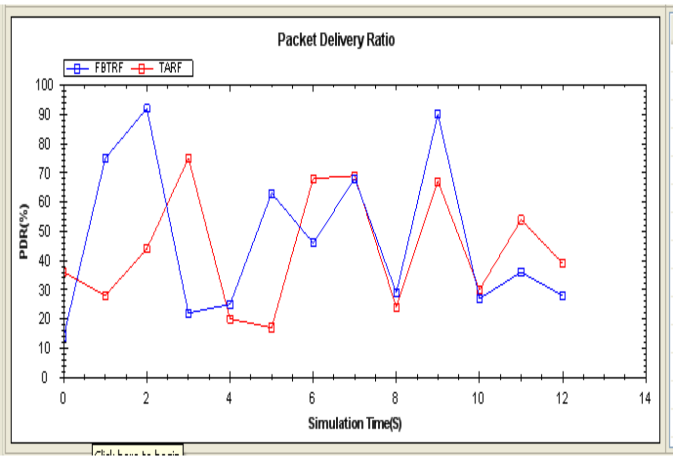


Fig.2. Performance Analysis: Packet Delivery Ratio

C. Throughput

The simulation analysis shown in the below snapshot shows the throughput efficiency. Throughput is defined as number of packets received by the sink successfully. Here the graph is plot between simulation time of 16 sec as a X-axis and No. of packet ratio as Y-axis. In this two protocol values are compared and proposed technique shows better results.

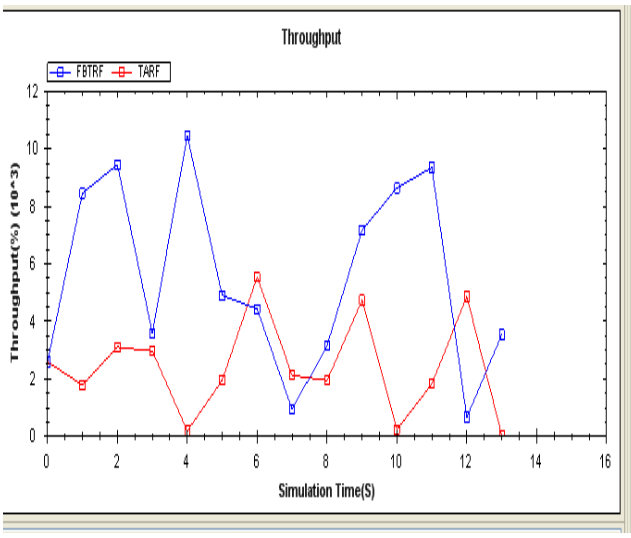
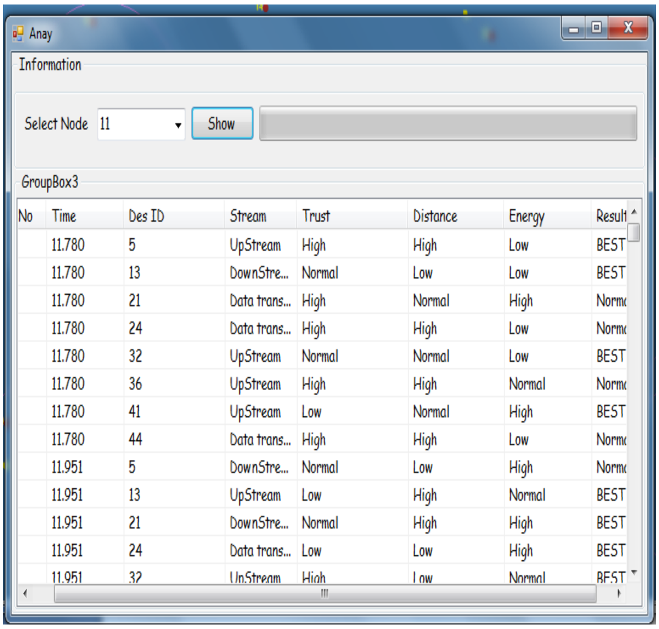


Fig.3. Performance Analysis: Throughput

D. Fuzzy Rule Table

Below snapshot is for fuzzy system.
Here the select node tab will select a source node and show Destination id, stream, trust value, its distance and energy.
On the basis of result it selects a node to route data packet to its destination.



No	Time	Des ID	Stream	Trust	Distance	Energy	Result
	11.780	5	UpStream	High	High	Low	BEST
	11.780	13	DownStre...	Normal	Low	Low	BEST
	11.780	21	Data trans...	High	Normal	High	Normc
	11.780	24	Data trans...	High	High	Low	Normc
	11.780	32	UpStream	Normal	Normal	Low	BEST
	11.780	36	UpStream	High	High	Normal	Normc
	11.780	41	UpStream	Low	Normal	High	BEST
	11.780	44	Data trans...	High	High	Low	Normc
	11.951	5	DownStre...	Normal	Low	High	Normc
	11.951	13	UpStream	Low	High	Normal	BEST
	11.951	21	DownStre...	Normal	High	High	BEST
	11.951	24	Data trans...	Low	Low	High	BEST
	11.951	32	UpStream	High	Low	Normal	BEST

Fig.4. Fuzzy System

VII. Simulation Parameter

No of nodes	50
Area Size	1500*1500
Simulation time	100s
Routing protocol	AODV
Mac	802.11
Packet Size	102…..512 bytes
Transmission range	250m
Misbehaving nodes	3
Number of Cluster	5

VIII. Conclusion

In this, trust based routing protocols are discussed. To overcome the drawbacks of existing method a trust based model using fuzzy logic is introduced that enables a node to keep track of the trustworthiness of its neighbours which provides reliable and secure routing in wireless sensor network. This technique effectively protects the wireless sensor network from replaying arouting information and from severe attacks.

Acknowledgement

The work presented in this paper is supported by G.H. Raisoni College of Engineering, Nagpur. Ms. A.V Sakhare is corresponding supportive author.

References

[1] Guoxing Zhan, Weisong Shi,"Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs, IEEE Transaction on dependable and secure computing, vol. 9, no. 2, 2012

[2] F. Akyildiz, W. Su, Y. Sankara subramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002. work,"

[3] Z. Cao, J.Hu, Z. Chen, M. Xu , and X. Zhou, "FBSR: Feedback-Based Secure Routing Protocol for Wireless Sensor Networks," Int'l J. Pervasive Computing and Comm., vol. 4, pp. 61-76, 2008.

[4] A. Rezgui and M. Eltoweissy, "Tarp: A Trust-Aware Routing Protocol for Sensor-Actuator Networks," Proc. IEEE Int'l Conf. Mobile Adhoc and Sensor Systems (MASS '07), 2007.

[4] J.L.X. Li and M.R. Lyu, "Taodv: A Trusted Aodv Routing Protocol for Mobile Ad Hoc Networks," Proc. Aerospace Conf., 2004

[5] T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, I. Papaefstathiou, C. Vangelatos, and L. Besson, "Design and Implementation of a Trust Aware Routing Protocol for Large WSNs," Int'l J. Network Security and Its Applications, vol. 2, no. 3, pp. 52-68, July 2010.

[6] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P.Levis, "Collection Tree Protocol," Proc. Seventh ACM Conf. Embedded Networked Sensor Systems (SenSys '09), pp. 1-14, 2009.

[7] Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victorwen And David E. Culler "SPINS: Security Protocols for Sensor Networks" ACM Journal of Wireless Networks, 8:5, September 2002, pp. 521-534.

[9] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. First IEEE Int'l Workshop Sensor Network Protocols and Applications, 2003.

[10] J. Al-Karaki and A. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," Wireless Comm., vol. 11, no. 6, pp. 6-28, Dec. 2004.

[11] F. Zhao and L. Guibas, Wireless Sensor Networks: An Information Processing Approach. Morgan Kaufmann, 2004. [3]

A. Wood and J. Stankovic, “Denial of Service in Sensor Networks,” Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.

[12] C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Proc. First IEEE Int’l Workshop Sensor Network Protocols and Applications, 2003.

[13] M. Jain and H. Kandwal, “A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks,” Proc. Int’l Conference.

[14] S. Buchegger and 1.-Y. L. Boudec, "Nodes bearing grudges: Towards routing security, fairness. And robustness in mobile ad hoc networks", in Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing,2002.

[15] S. Ganeriwal, L. Balzano, and M. Srivastava, “Reputation-Base Framework for High Integrity Sensor Networks,” ACM Trans.Sensor Networks, vol. 4, pp. 1-37 2008.

[16] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks,” IEEE Comm. Magazine, vol. 40, no. 8,pp. 102-114, Aug. 2002..

[11]F. Zhao and L. Guibas, Wireless Sensor Networks: An Information Processing Approach. Morgan Kaufmann, 2004. [3] A. Wood and J. Stankovic, “Denial of Service in Sensor Networks,” Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.

[12] C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Proc. First IEEE Int’l Workshop Sensor Network Protocols and Applications, 2003.

[13] M. Jain and H. Kandwal, “A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks,” Proc. Int’l Conference.