Research of Various Techniques for Evaluating Nodal Trust in Hierarchical WSN

Aarti K. Naryani, Rachana Deshmukh, Rashmi Deshmukh

Abstract—In today's modern world the wireless sensor networks have become a crucial tool to serve various purposes. The applications falling in range of wireless sensor networks are vast and tend to conquer our everyday life. It was initially designed for surveillance and monitoring for defense related operations but then it also proved to be boon for the health, traffic, consumer and industrial areas. Also, it is one of the most popular technologies for smart cities. However, the wireless sensor networks are highly prone to security attacks, and due to the dynamic, collective and collaborative behavior of sensor networks a secure data transfer has become a challenging task. The deployed sensor nodes, especially in the multi hop environment can get compromised and can behave maliciously. Therefore it becomes necessary to assess the trust worthiness or reliance of the sensor node over the other present in the network. Several researches have investigated various techniques for determining the nodal trust in WSN. This paper discusses the major challenges in wireless sensor network, potential attacks occurring due to compromised nodes along with the different types of trust models. It also figures out some of the existing trust models which are used in evaluating nodal trust in wireless sensor networks.`

Index Terms— Wireless sensor networks, trust model, compromised nodes, attacks.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have been recognized as one of the most important technologies for the twenty - first century [1]. Its distinguished characteristics, such as remote and denser level of node deployment, high degree of unreliability of sensor nodes, severe energy computation, and storage limitations makes it different from traditional wireless communication networks, such as, cellular systems and MANET i.e. mobile ad hoc networks. This however, introduces the different set of challenges in the development and application of WSNs. The Fig I show the structure of a typical sensor node. In the past decade, looking to the popularity of WSNs, it had become the favorite topic all over the globe both in the field of industry and academia. Various researches have been carried out to traverse and solve various issues related to design and application of WSN. Significant advances have been made in the remote deployment and development of WS nodes.

In the near future WSNs will be widely used in various domestic and military fields, and transform the way we perform the usual activities in the physical world.

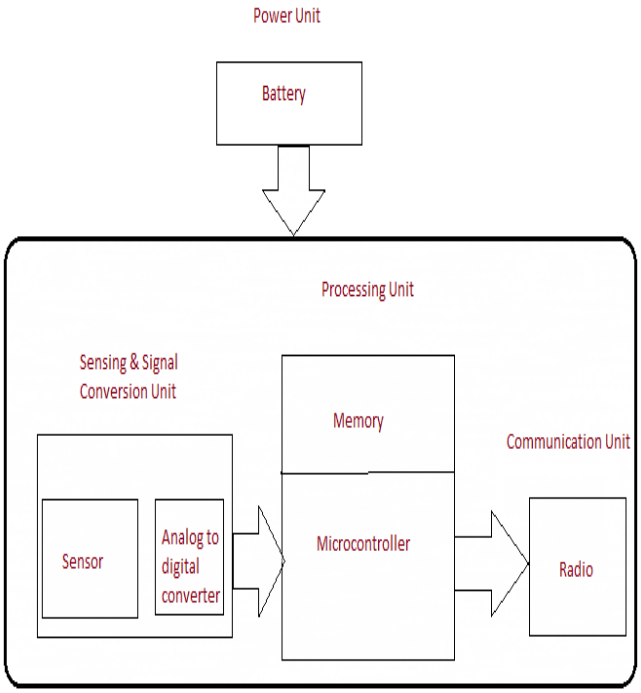

Fig I. The structure of the typical sensor node

II. WIRELESS SENSOR NETWORK CHALLENGES

The WSNs possesses the unique network characteristics. The- refore, the design of WSN presents many challenges, whichcovers the following main aspects:

• **Energy Constraints**: Sensor nodes are battery operated and lack the automatic recharging capability. Data collection [3], processing and communication, continuous listening to the medium for packet receiving and transfer everything requires large amount of energy.

•**Limited Hardware and Software Resources:**It has limited processing and storage capacities, and thus can only perform limited computational functionalities [4].

• **Massive and Random Deployment:** The sensor nodes are deployed remotely and are expected to autonomously organize, configure, adapt, maintain and repair themselves [5] in a hostile environment.

• **Dynamic and Unreliable Environment:** The network connectivity between the sensor nodes may be frequently disrupted because of channel fading or signal attenuation [1].

•

Revised Version Manuscript Received on 16 September, 2019.

Prof. Aarti K. Naryani, G. H. Raisoni University, Madhya Pradesh, India.
(Email: Aarti.naryani786@gmail.com)
Prof. RachanaDeshmukh, G. H. Raisoni University, Madhya Pradesh, India.
(Email: rachana1509@gmail.com)
Prof. RashmiDeshmukh, Priyadarshini Indira Gandhi College of Engineering, Maharashtra., India.
(Email: rashmi_deshmukh86@yahoo.co.in)

Security: Security services have been provided such as Link-layer encryption and authentication, Identity verification, Bidirectional link verification, etc. but the specific technique cannot resist all types of attacks [6].

• **Diverse Applications:** It is difficult to build a protocol which can fulfil all the requirements of all the applications, since the design of sensor networks is application specific. The new middleware for WSNs, called Motley middleware [10], have made it possible to some extend to support diverse applications in shared infrastructure environment of WSNs.

III. MOTIVATION FOR TRUST MANAGEMENT IN WSN

From the above mentioned challenges one can determine the level of unpredictable environment of sensor networks. This gives attackers the very chance to perform anonymous changes in sensor nodes. Trust of a sensor node is one of the most important categories of Intrusion Detection System in WSN [2]. There are basically, two types of nodes in the network- trustworthy nodes and untrustworthy nodes. The trustworthy nodes forward the network traffic towards the destination node dedicatedly, sincerely and cooperatively. On the other hand, untrustworthy nodes are the compromised node. A compromised node is a node which after remote deployment of sensor nodes may exhibit unpredictable behavior and may cooperate in a secret or unlawful way with other compromised nodes in order to gain an advantage over others trustworthy nodes present in the network [7]. Generally node compromise occurs when an intruder captures a node, and then that is directly connected to their machine through a wired or wireless connection. Then, the original programming of that node is replaced with some sort of destructive programming and then that node is set in the network with other sensor nodes as it was previously. This node can be used by the attacker to launch more serious attacks. The untrustworthy node act according to the instructions provided by the intruder and thus behaves very suspiciously, maliciously and selfishly. It may direct the traffic to the adversary node or flood the packets by creating too much duplication or modify the contents of the message. Several widely known attacks like wormhole, Sybil, black hole, gray hole, DoS, replay etc [8] target the nodes thereby destroying the complete network.

IV. NODE COMPROMISE POTENTIAL ATTACKS

In the following section, Table I attempts to list as many attacks as possible that may occur due to node compromise.

A. Trust Model

The trust model supports the trustworthy nodes to communicate among them and discourages untrustworthy nodes to participate in the network activities. Using trust models one can obtain the trust related information which can define each node's trustworthiness. The network lifetime, toughness and throughput depend on number of trustworthy nodes present in the network. A trust model plays important role not only in the higher level of decisions such as routing [22] and data aggregation [23], but also cluster head election and, and key distribution [24]. Trust model performs network monitoring activities thereby increasing the security. Also, it minimizes the risk and ensures good performance of activities such as data gathering and data processing [25]. In this paper, we surveyed and examined the already proposed trust models and studied their advantages and disadvantages. Our purpose is to enlist useful guidelines for the design of trust models that can be implemented in real-life applications.

The trust models can be distinguished in three categories centralized, hierarchical and distributed [26] depending on which node in the remotely deployed sensor network carries out the responsibility of evaluating and analyzing the trust values of other nodes. In the centralized case [27], the sink node or the head node is considered to be the most trusted node and it is responsible for examining the trustworthiness of its surrounded sensor nodes. The trust values are calculated on the basis of the parameters values collected by sink node on its own, or values received by all or specific nodes in the deployed sensor network. This head node then broadcasts these trust values in the network so that the nodes can use it to make their decisions. The advantage of announcing the trust values to network is that there individual node need not be equipped with this functionality. But then this comes with two severe disadvantages. First, percolating the trust information in the network needs extra energy consumption and second, trust information is with individual node if this node is compromised then it could lead to severe network disruption. Centralized trust model fails in case of denser sensor nodes deployment and resource limitations. The hierarchical trust model [28] overcomes the limitations of centralized trust model. In hierarchical trust model, there are group of clusters and each cluster has Cluster Head (CH) which takes the responsibility of computing the trust of nodes in its kingdom. In distributed nodal trust each node is monitoring all its neighboring nodes and individual nodes assess the trustworthiness of its neighbors. This forms a distributed trust architecture [29].

V. RELATED WORK

A. Determining Nodal Trust in Hierarchical WSN

The table (Table III) lists various techniques presented by different researchers for evaluating the trustworthiness of the sensor node in hierarchical environment.

In paper [30], the researcher Idris M. Atakli proposed a weighted-trust evaluation (WTE) based scheme in order to identify the compromised nodes in hierarchical WSN by observing its reported data. This paper tries to identify mischievous node in spite of the so called Byzantine problem [30]. The Forwarding node aggregates the data send by the sensor nodes. Here, each sensor node is assigned weight W. The weight of each sensor node is likely to be decreased if it frequently sends the information that is conflicting with the final decision. Finally, the node is detected as the malicious node as its weight goes down the specific weight. With respect to the mismatch among response time, detection and mis-detection rates, the weight penalties are also introduced.

In research [31], the sensor nodes are organized into number of clusters allocating each cluster with the cluster head. The trust values are calculated when it is requested.

Each sensor node is assessed by its cluster head on the basis of the report submitted by its neighboring nodes for the trust values and similarly, each cluster head is assessed by the base station on the basis of the report submitted by its neighboring cluster heads. The trust values are calculated on the basis of two factors QoS (Quality of Service) trust metrics (energy, unselfishness) and social trust metrics (honesty, intimacy). The trust values of sensor nodes are calculated on demand from CH and BS. The trust values in this paper are calculated same as HTM [35].

In another research [32], the trust management architecture for hierarchical WSN is proposed which evaluates the nodal trust with reduced computation and communication requirements. Here, all sensor nodes and the CH nodes are assumed to be static or motionless. Also, the physical locality and range of communication of all nodes is assumed to be known in the network. In this, the concept of direct, indirect and integrated trust is introduced along with the sponsor and target nodes. According to the paper, the sponsor node selects the target node on the basis of direct trust value of target node. The CH decides the group trust value on the basis of the trust values sent by individual sensor nodes of other nodes in the cluster. The trust information is calculated at various levels like cluster head level, intra and inter cluster heads level along with sponsor and target nodes trust level.

Attack		Description
Routing loop attacks		In this attack, the malicious nodes completely modify the routed packets so that packets enter a sort of loop (cycle) and could not reach the predetermined destination [9].
Wormhole attacks		In this type, a secret route is established by the attacker between two distant places bycompromising the group of destructive nodes and then the packet is diverted through that established channel [1][10].
Selective Forwarding	Grayhole	In this type of attack, the destructive nodes disallow the packets to pass through the in the network
	Blackhole	Black hole attack which is very complex to detect and defend. In this, an attacker gains the control of the sensor node(s) and re-programs them in order to block the data packets they receive and disallow them from forwarding to the intended destination [11].
	DoS attacks	In this type of attack, the intruder aims at making the machine or a complete network resource unuseful and unavailable to its predetermined users by temporarily or indefinitely discontinuing services of a server connected to the Internet [12].
Sinkhole attack		In this type of attack the malicious node pretends itself to be the most attractive one in terms of probably having a good trust level and a node having the tiny distance to the base station. In this way, by drawing attention of other nodes and by advertising itself, it takes part in the routing process and try to draw as many packets from this path as possible[12].
False information or false recommendation		The group of destructive node may work together to provide wrong information against the trustworthy nodes in order to spoil their reputation. Same happens in *stacking attack*, where the malicious nodes keep spreading false information about a peer node and create its negative reputation [13].
Incomplete information		A destructive node provides the improper and incomplete information. It always tends to mislead other nodes [11].
Packet modification/insertion		In this, the destructive node tries to modify the contents of the packet. Also inserts compromised packets with incorrect routing information in the network [15].
Sybil attacks		It is an attack in which multiple identities from same malicious node is created. This attack is very dangerous for WSN as it can act as the gateway for any other attacks such as wormhole, sinkhole, selective forwarding etc [17].
Blackmailing		A compromised node is able to blackmail another node by circulating wrong facts that another node is mischievous or malicious. This generates chaos in the network and disrupts the normal functioning of the whole network [18].
Replay attacks		This attack aims at sending outdated information in the network which can cause many problems [19]. An attacker captures a data packet from a sensor network, grip it for indefinite amount of time, and then send it into the network.
Selective misbehav-ing attacks	On-off attacks	In this, the malicious node behaves very unpredictably. Like it sometimes shows very good and cooperative behavior or sometimes behaves selfishly just to remain unidentified and undetected from its malicious activities [20].
	Conflicting behavior attacks	A destructive node behaves in different ways with different groups in the network and makes different opinions about other thus creating conflicts and groupism in the network ultimately resulting in the non-trusted relationships [21].
False Reports		Not every node in the network is able to send the data directly to the BS in order to avoid energy waste. So few nodes take the responsibility of aggregation of data from all nodes and clubbing that data by the process called data fusion and then generating the final report and transmitting a single report to the base station. However, if some malicious nodes get involved in the data fusion process then false report will be sent to the BS.

Table I. Potential attacks occurring due to node compromise

Riaz Ahmed Sheikh, in his research paper [33] stated a new lightweight technique called Group-Based Trust Management Scheme (GTMS) for Clustered Wireless SensorNetworks. It is an intrusion tolerant technique that helps in detecting and preventing malicious, egocentric, and defective nodes by using hybrid trust management approach. GTMS computes the trust values of sensor nodes based on direct or indirect observations. The trust is calculated at three different levels-node level, Cluster level and Base station level. In this, it is assumed that all SNs have typical unique identities like location, node type, and node subtype. The research paper proposes a trust model which works with two different topologies intragroup & intergroup.

In yet another research work proposed (HTECH) [34], an efficient method of selection of CH based on trust routing is demonstrated. Trust Design process considers four parameters such as node generousness (unselfishness), Node Cooperativeness, Node Biasness (Honesty) and Node Data Transmission Rate on the basis of which the trust is evaluated. The cluster head is selected on the basis of Trust value. According to the author, this protocol performs ideally in terms decrease in delay and delivery rate.

In [35], considers two factors for assessing trustworthiness, namely social trust and QoS trust. It is a probability model using stochastic Petri nets techniques which analyzes the protocol performance with respect to its quantities, and validating subjective trust against objective trust calculated based on actual status of nodes.

TBHR Protocol for WSN [36], is concerned with the energy conservation of the network. It is basically designed for multi-hop hierarchical wireless sensor network. It evaluates the trust value for individual sensor node in the n/w on the basis of the components derived from communication and social networks. In this paper, the residual energy or leftover energy of the node and its number of negotiations with the neighbors and CH are considered as the basis for trust evaluation.

The following table (Table II) elaborates in general the merits and demerits of the above described nodal trust technologies

Technique Used	Merits	Demerits
WEIGHTED TRUST EVALUATION TECHNOLOGY [30]	-It is easier and less complicated to keep track of the nodes and it is difficult to gain control over most of the node unless an attacker gains control of the base stations. -This approach is best suited for small and dense sensor networks.	-The whole system will fail if the BS itself gets compromised. -If the quantity of the compromised nodes leads the legal nodes, then the legal nodes will be reported as malicious.
RHTM [31]	-It calculates the trust values of Sensor nodes and CH on request only thereby reduces the energy consumption rate of sensor nodes.	This scheme cannot identify those types of attacks in which the attackers gives false recommend - ations about the other nodes but then forwards the packet correctly
TMA [32]	- Suitable for aggressive node movement and multi-hop routing - It uses timing window and a decay function in order to assess the changing behavior of trust in trust calculations.	Static assumptions are made
GTMS [33]	- Reduces the cost of trust evaluation - Suitable for large scale networks	-Memory overhead for Nodes is more compared to TMA - Not suitable for dynamic node movement and multi-hop routing
HTECH [34] & HTM [35]	- As per the simulation results HTECH decreases both packet loss rate, delay rate, and improves output of SNs and shows Performance close to the expected performance with regards to energy consumption. - HTM Shows expected performance level that is achievable by routing based on flooding in message delivery ratio andout performs the traditional routing protocols that do not make use of trust concept in selective forwarding of nodes in message delivery.	-
TBHR [36]	-Improves network lifetime by allowing more number of nodes to take part in transmission to achieve stability in energy in the nodes. -Results indicate that it performs around 10 % better than TBGR scheme with respect to network lifetime and approx. 5% better than AODV protocol when packet delivery ratio is considered.	-In this, the end-to-end delay in when packet is forwarded from S to D in the network is more.

Table II. Merits and Demerits of different nodal trust evaluating hierarchical WSN Techniques

VI. COMPARATIVE ANALYSIS OF HIERARCHICAL TECHNIQUES& RESULTS

ThecomparativeanalysisofHierarchicalnodaltrusttechniquesdescribedabove is discussed in the following table (Table III).

Specification	RHTM	TMA	GTMS	WTE	HTECH	HTM	TBHR
Calculation of trust value of nodes	On Demand	Recorded	Recorded	Recorded	Recorded	Static	Static
Energy Consumption Consideration	Yes(Consumes 6K J in 100 sec	Yes	Yes (Consumes 10K J in 100 sec)	No	9.5J residual energy is left after 50ms	Yes (Consumes 8K J in 100 sec)	Yes (Amount of residual energy left is considered)
Node Movements	Static	Dynamic	Static	Static	Static	Static	Static
Communication overhead consideration	No	Yes	Yes	Yes	No	Yes	No
Storage overhead consideration	No	Yes	Yes	Yes	No	Yes	No
Memory overhead consideration	No	No	Yes	Yes	No	Yes	No
Computation overhead consideration	No	Yes	No	No	No	Yes	No
Trust Decay consideration	No	Yes	Yes	No	No	Yes	Yes

Table III. Comparative analysis of various hierarchical techniques

VII. CONCLUSION

This paper extensively discusses the major challenges and the potential attacks that can occur in WSN due to sensor node compromise. Many researchers have proposed several techniques and mechanisms to cope up with the severe vulnerabilities caused due to malicious node in WSN. This paper tried to explore the researches done in the field of detecting and isolating the compromised nodes causing danger to the network. This can be helpful to the researchers who are working on node compromise attacks either in centralized or hierarchical wireless sensor network.

REFERENCES

1. Jun Zheng, Abbas Jamalipour, "Wireless Sensor Networks - A networking Perespective", IEEE, A John Wiley & Sons, Inc. Publication ISBN-978-0-470-16763-2
2. Audrey A. Gendreau, Michael Moorman, "Survey of Intrusion Detection Systems towards an End to End Secure Internet of Things", IEEE 4th ICFITC, 978-1-5090-4052-0/16 © 2016 IEEE
3. M. H. Anisi, A. H. Abdullah, and S. A. Razak, "Energy-Efficient Data Collection in Wireless Sensor Networks", 2011 WSN, pp. 329-333, vol. 3.
4. A. Crenjin, "Software Issues in Wireless Sensor Networks", WSN: concepts, multidisciplinary issues and case studies, Belgrade, 2009, pp. 1-9.
5. K. Sohrabi, J. Gao, V. Ailawadhi, G. J. Pottie, "Protocols forself organization of a wireless sensor networks", Personal Communications IEEE, vol. 7, Issue 5, 2000, pp. 16-27.
6. P. Mohanty, S. Panigrahi, N. Sarma, "Security Issues In WSN Data Gathering Protocols: A Survey", Journal of Theoretical and Applied Information Technology, volume 13, Issue 1, 2005-2010, pp. 14-27.
7. www.igi-globeal.com...promised-node/4960
8. Yuxin Liu, Mianxiong Dong, Member, IEEE, Kaoru Ota, Member, IEEE, and Anfeng Liu, "Active Trust: Secure and Trustable Routing in WSN", IEEE Transactions On Information Forensics And Security, Volume 11, Issue No. 9, Sept. 2016.
9. J. Chen, B. Wu, , J. Wu, M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless Network Security-Signals and Communication Technology, Part II, 2007, pp.103-135, Springer U.S.
10. R. Maheshwari and S. R. JieGao Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," Published in Proceedings of 26th IEEE Int'l Conf. on Computer Communications, May'07 , pp. 107-115.

11. GursheenKaur, Mandeep Singh, "Detection of Black Hole in WSN based on Data Mining", 5th Int'l Conf. on "Confluence The Next Generation Information Technology Summit "IEEE Yr 2014,78-1-4799-4236-7/14
12. https://s2.ist.psu.edu/paper/ddos-chap-gu-june-07.pdf
13. Various Attacks in WSN: Survey K. Venkatraman, J. Vijay Daniel, Int'l Journal of Soft Computing and Engg. (IJSCE) ISSN: 2231-2307, Vol-3, No.1, Mar'13
14. W. J. Adams, G. C. Hadjichristof, "Calculating a Node's Reputation in a Mobile Ad Hoc Network," Published in Proceedings of 24th IEEE Int'l Performance Computing and CommConf, Phoenix, AX, 7-9 Apr'05, pp. 303-307
15. L. Capra, "Toward a Human Trust Model for Mobile Ad-hoc Networks," Published in Proceedings of 2nd UK-UbiNet Workshop, May'04, Cambridge University, UK.
16. Jin-Hee Cho, Ananthram Swami, "A Survey on Trust Management for Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials, Volume. 13, Issue 4, 4th Quarter'11
17. Abirami K#1, Santhi B*2 "Sybil attack in Wireless Sensor Network", Int'l Journal of Engg and Tech. (IJET), ISSN : 0975-4024 Volume 5. Issue 2, May'13
18. Z. Liu, A. W. Joy, "A Dynamic Trust Model for Mobile Ad Hoc Networks", Published in Proceedings of 10th IEEE International W/shop on Future Trends of Distributed Computing Systems, China, May'04, pp. 80-85
19. N. Bhalaji and A. Shanmugam, "Reliable Routing against Selective Packet Drop Attack in DSR based MANET", Journal of Software, volume 4, Issue 6, Aug'09, pp. 536-543.
20. N. Bhalaji and A. Shanmugam, "Reliable Routing against Selective Packet Drop Attack in DSR based MANET," Journal of Software, vol.4, no. 6, Aug'09, pp. 536-543.
21. J. Li, R. Li, and J. Kato, "Future Trust Management Framework for Mobile Ad Hoc Networks: Security in Mobile Ad Hoc Networks", IEEE Commun. Mag., volume 46, Issue 4, April '08, pp. 108-114.
22. E. Aivaloglou and S. Gritzalis, "Hybrid trust and reputation management for sensor networks", Wireless Networks, volume 16, Issue 5, pp. 1493–1510, Jul'10.
23. Wei Zhang, Sajal K. Das, "A Trust Based Framework for Secure Data Aggregation in WSN", IEEE Commun. Society on Sensor Ad Hoc Communications and N/wks, 1, 60-69, 2006.
24. Theodore Zahariadis, Helen C. Leligou1, Panagiotis Trakadas2 and Stamatis Voliotis1, "Trust management in WSN" Eur. Trans. Telecomms. 2010; 21:386–395DOI: 10.1002/ett Published online Apr'10 in Wiley Inter Sci.
25. V. Uma Rani, K. Soma Sundaram, "Review of Trust Models in WSN", World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Info Engg. Vol:8, No:2, 2014
26. Theodore Zahariadis1, Helen C. Leligou1∗, "Trust management in wireless sensor networks", EUROPEAN TRANSACTIONS ON TELECOMMUNICATIONS Eur. Trans. Telecomms. 2010; 21:386–395 Published online 8 April 2010 in Wiley Inter Science (www.interscience.wiley.com)
27. Tanachaiwiwat S, Dave P, Bhindwale R, Helmy, "A Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks", IEEE International Conference on Performance, Computing, and Communications, Phoenix, AZ, USA, 2004.
28. Crosby G V, Pissinou N., "Cluster-based reputation and trust for wireless sensor networks" Consumer Communications and Networking Conference, Las Vegas, NV, USA, 2007.
29. Mahdi Abdulkader Salem, "An Efficient Distributed Trust Model for Wireless Sensor Networks",Issue No:5(May) research ISSN No:2348-4845.
30. Idris M. Atakli, Hongbing Hu, Yu Chen*, Wei-Shinn Ku, Zhou Su, "Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation", 2008 SpringSim 1-56555-319-5
31. Reshmi V1, Sajitha M2, "A Reactive Hierarchical Trust Management Scheme for Wireless Sensor Networks (RHTM)", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 03 Issue 07 July, 2014 Page No. 6982-6984
32. Junqi Zhang1, Rajan Shankaran1, Mehmet A. Orgun1, Vijay Varadharajan1 and Abdul Sattar2, "A Trust Management Architecture for Hierarchical Wireless Sensor Networks", 35th Annual IEEE Conference on Local Computer Networks, 978-1-4244-8388-4/10/$26.00 ©2010 IEEE (TMA)
33. R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. L. and Young Jae Song, "Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks (GTMS), IEEE Trans. Parallel and Distrib. Sys, vol. 20, pp.1698–1712, 2009.
34. L. Ramalingam1* and S. Audithan2, " Design of Hierarchical Trust based Efficient Cluster Head Selection in WSN (HTECH)" Indian Journal of Science and Technology, Vol 9(26), 10.17485/ijst/2016/v9i26/90074, July 2016 ISSN (Online) : 0974-5645
35. FenyeBao, Ing-Ray Chen, Moonjeong Chang Jin-Hee Cho," Hierarchical Trust Management for Wireless Sensor Networks and Its Application to Trust-Based Routing" SAC'11, March 21-25, 2011, TaiChung, Taiwan
36. Yamuna Devi C Ra, SaishivaKa, Sunil Kumara, S H Manjulaa, K R Venugopala, L M Patnaikb, "Trust-Based Hierarchical Routing Protocol for Wireless Sensor Networks" International Journal of Information Processing, 9(1), 101-112, 2015 ISSN : 0973-8215