ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Trust Aware Secure Routing for Cluster-based Wireless Sensor Networks - A Comparative Study

P.Prittopaul[1], Dr.N.Shankarram[2]

Research Scholar, Dept. of Computer Science, Velammal Engineering College, India[1]

Prof &Head, Dept. of Computer Science &Engg, RMK College of Engg &Tech Chennai, India[2]

ABSTRACT- As wireless sensor networks *is* a self organizing and infrastructure less network in nature they are subject to various types of attacks on various environments. The objective of this paper is to mainly focus on a trust aware model between the communicating sensor nodes and the base station. A cluster node aggregates the data from other sensor nodes and eradicates the disused data, disseminates the used data to the base stations that are one hop distance from the node. Since base stations acts as an interface between the communicating sensor devices, the nodes are subject to various attacks on various layers. Here a comparative study is made on various types of attacks on a clustered environment and little available trust aware models are also discussed that defence against the various types of attacks that induces harm between the sensor nodes and base stations.

KEYWORDS— Wireless Sensor Networks, Dissemination, Trust Management.

I. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location(base station). The development of wireless sensor networks was motivated by military applications such as battlefield surveillance [1]; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

Sensor Networks are highly distributed networks of small, trivial wireless nodes, deployed in large numbers to monitor the environment or system[2]. Wireless sensor networks are getting hold of popularity due to its low cost. These sensor nodes are data centric, which means the nodes are addressed by some queries either by other nodes or by base station. The query is addressed to all nodes based on some condition. Since data are to be gathered and disseminated among sensors they are vulnerable to various attacks on various layers. Even though many researchers have discussed about various types of attacks, still reasonable solutions are not provided due to the adhoc nature of the node. In this paper we have made a survey on various types of attacks that occurs on a sensor network within and outside the base station. On account of saving energy, some nodes may act as a selfish node by not forwarding the packets to sink node or base station. Few other sorts of attacks like

In section 1 we discuss about the various types of attacks in WSN. It also focuses on the attacks that arise between the sensor nodes to base station. In section 2 we have discussed about some threats to sensor network in clustered base environment and in section 3 we have made a comparative study of Trust aware routing models to provide trust between sensor nodes and base station in cluster based environment.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

1. Threats in WSNs.

TABLE 1. TYPICAL THREATS IN WSNS

Threat	Layer	Security Techniques
Jamming	Physical	Spread-Spectrum, lower duty cycle, priority messages, region mapping, mode change
Tampering		Tamper-proofing, hiding, effective key management schemes
Exhausting	Link	Rate limitation
Collision		Error correcting code
Unfairness		Small frames
Neglect and Greed	Network	Redundancy, probing
Homing		Encryption
Misdirection		Egress filtering, authorization, monitoring
Black holes		Authorization, monitoring, redundancy
Flooding	Transport	Limiting connection numbers, client puzzles
Desynchronization		Authentication
Clone Attack	Application	Unique pair-wise keys

There are a few more attacks in which adversaries misdirect network traffic by identity deception through replaying routing information. Such attacks are selective forwarding, wormhole attacks, sinkhole attacks, Sybil attacks and HELLO flood attacks [3].

Selective Forwarding

In a selective forwarding attack, malicious nodes decline to forward packets and make sure that they are not propagating further. This type of attack will not always happen on the data flow but also on controlling packets such as HELLO packets or acknowledgement packets. Selective Forwarding relies on the routing methodology. It involves subverting a node on a major traffic path.. Counter measures include redundant routes and redundant messages.

Worm hole attacks

Even if the malicious node cannot directly overhear the valid node's wireless transmission, it can collude with other malicious nodes to receive those routing packets and replay them somewhere far away from the original valid node, which is known as a wormhole attack [4].Once a wormhole is established, malicious nodes can use it to make a Denial-of-Service attack by, for instance, dropping certain data or control packets. To launch a wormhole attack, an adversary establishes a direct link referred as wormhole link between two points in the link. Once the wormhole link is operational, the adversary eavesdrop messages at one end, referred as the origin point, tunnel them through the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

wormhole link and replays them in a timely fashion at the other end, namely the destination point. It is often difficult to know whether a node forwards received packet correctly even with overhearing techniques [3].

Sinkhole attack

Here a malicious node may claim itself to be a base station through replaying all the packets from a real base station [5]. In a Sinkhole attack the opponent's goal is to tempt almost all the traffic from a meticulous area through a compromised node. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm.[16].

Sybil attack

The same sink hole attack can be employed to conduct another strong form of attack [6] called the Sybil attack – where the attacker tries to forge multiple identification in a certain region. By broadcasting messages with multiple identifications, a sybil node can rig the vote on group based decisions and also disrupt network middleware services severely.

Hello flood attack

In HELLO flood attack, new sensor nodes broadcast "hello" to find its neighbours. The sensor nodes also broadcast its route to the base station. Other nodes may choose to route data through this new node if the path is shorter. Adversary node broadcast a short path to the base station using a high power transmission. Target nodes attempt to reply, but the adversary node is out of range. This attack puts the network in a state of confusion. This attack can be countered by using a three-way handshake. New node sends HELLO and any receiving nodes reply with randomly generated message. The new node must resend the message back to the receiving nodes. This guarantees the bi-directionality of the link.

II **CLUSTERED BASED WIRELESS SENSOR NETWORKS**

The clustering phenomenon as we can see, plays an important role in not just organization of the network, but can dramatically affect network performance. The nodes of a wireless network are divided into several disjoint or overlapping clusters [9]. Each cluster elects one node as the so-called "cluster head". These special nodes are responsible for the routing process. Cluster heads are able to communicate with each other using gateway nodes. A gateway is a node that has two or more cluster heads as its neighbors or when the clusters are disjoint, at least one cluster head and another gateway node. Due to the clustered structure, there will be less traffic, because the route requests will only be passed between cluster heads. Identifier based clustering is a better choice than connectivity based clustering according to node movement. In order to support the cluster formation process, each node uses a neighbour table, where it stores information about its neighbour nodes, such as their ID's, their role in the cluster and the status of the link to that node. Many sensor network routing protocols are quite simple, and for this reason are sometimes even more susceptible to attacks [10]. Most network layer attacks against sensor networks include Spoofed, altered, or replayed routing information, Selective forwarding, Sinkhole attacks, Sybil attacks, Wormholes, HELLO flood attacks, Acknowledgement spoofing. The description of each kind of attack is given in [3]. Also the countermeasures and limitations are discussed in [3]. Typical security attacks and their behaviour is shown in Table II.

TABLE 2. NETWORK LAYER ATTACKS AND BEHAVIOUR

Attack type	Attacker behaviour
Selfish behaviour (black-hole, greyhole)	A malicious node denies to perform benign routing and drops part or all the received packets.
Sinkhole Attack	A malicious node tries to attract traffic advertising fake routing information, and then it refuses to forward it.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Replay attack	The original routing messages are repeated at a later time, thus deceiving the routing functionality.
Link Spoofing Attack	An adversary can spoof link layer acknowledgement for overheard packets to convince the sender that the packet has been forwarded successfully.
Modification attack	An adversary modifies the data and/or routing packets it forwards.
Sybil attack	An attacker presents multiple Identities

A method of key establishment characterized by the fact that no secure channels are needed, and, more important, no party is allowed to choose the key on behalf of the group [11]. In other words, the group members don't trust each other. This strong but much realistic requirement provides background and motivation for considering malicious participants in such protocols and for defining in a formal way what security means in that case. Each security group may have its own security requirements concerning access control, communication, information storage and processing which include Confidentiality, Authentication and Integrity [12]. One of the main techniques to achieve this is cryptography. Group Key Establishment is a process or protocol whereby a shared secret becomes available to two or more parties for subsequent cryptographic use. It falls into two classes- Group Key Transport/Distribution and Group Key Exchange/Agreement. Group Key Transport/Distribution is a group key establishment technique where one party creates or otherwise obtains a secret value, and securely transfers it to others. Group Key is chosen by a single party and then securely transferred to all group members. Group Key Exchange/Agreement is a group key establishment technique in which a shared secret is derived by two or more parties as a function of the information contributed by, or associated with, each of these, such that no party can predetermine the resulting value. All group members have to interact in order to compute the group key. The main difference to group key transport is that no party is allowed to choose the group key on behalf of the whole group.

Generally, routing protocols on the basis of network structure are divided in to 3 main groups:

1. flat
2. hierarchical
3. location based

Specifically, hierarchical routing protocols have proved to have considerable savings in total energy consumption of the WSN [8]. In hierarchical routing protocols, clusters are created and a head node is assigned to each cluster. The head nodes are the leaders of their groups having responsibilities like collection and aggregate the data from their respective clusters and transmitting the aggregated data to the BS. This data aggregation in the head nodes greatly reduces energy consumption in the network by minimizing the total data messages to be sent to BS. The less the energy consumption, the more the network life time. The main idea of developing cluster-based routing protocols is to reduce the network traffic toward the sink. This method of clustering may introduce overhead due to the cluster configuration and maintenance, but it has been demonstrated that cluster-based protocols exhibit better energy consumption and performance when compared to flat network topologies for large-scale WSNs.

III TRUST AWARE ROUTING ALGORITHMS IN WSN

Trust Management in wireless sensor network is a current challenging issues in recent years for researchers as deploying wireless sensor network in large scale is highly a complicated task hence sensor networks are subject to various attacks like denial of service attack, routing attack, malicious node attack to name a few. Various cryptographic techniques can be used to overcome these attacks but still this leads to high cost and more overhead. As a solution to this, various trust management schemes have been introduced which provides a trusted relationship between the communicating nodes either with the sink or with the base station. One of the main existing feature of WSN is it can be deployed without any infrastructure. The sensor nodes mainly rely on the neighbouring nodes to provide a route towards the sink or base station. In case of cluster nodes the cluster head act as a gate way to other clusters or base

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

station. Hence, trust establishment among the nodes is mandatorily required to evaluate the trustworthiness of other nodes.

Due to some challenges, many new algorithms have been proposed for the routing problem in WSNs. In [15][16] it has been explored some of the routing techniques in WSNs that have been developed in recent years.

TABLE 3. TRUST AWARE ROUTING ALGORITHMS AND TECHNIQUES

Routing algorithm	Technique Employed
Trusted AODV	A trust information exchange mechanism
Trust Aware Dynamic Source Routing	A mechanism involving the "watchdog" and "pathrater" modules
TGPSR	It is enhanced to take node trust levels into account.
TRANS	Blacklisting is distributed by the sink
Trusted cluster head election	The new cluster head is elected based on the majority of votes
Cluster based trust – aware routing protocol(CBTRP)	The routed packets are cosseted from malicious nodes by attempting to route only through trusted nodes
TARF	Evaluates the trustworthiness of neighbouring nodes.
ATSR	Relies on a distributed trust model for the detection of malicious nodes

3.1Trusted AODV

TAODV [15] protocol suggest a trust relationship among nodes and hence malicious nodes are detected and shorn of to the entire network. It does on rely on public key cryptography or trusted third parties which lead to more computational overhead. Rather few trust models are proposed to find out the neighbour nodes and build a trust relationship among the communicating nodes. Trusted AODV uses self organized key management mechanisms to build a trust relationship between nodes. Hence it knows the neighbouring details by using the sequence number and unique ID between nodes.

3.2Trust aware dynamic source routing

DSR is an "On-Demand" routing protocol which executes the path finding process and exchange the routing information only when the path is required [20]. TDSR relies on Watch Dog and Pathrater for trusted communication between nodes. Watch dog is used to monitor the malicious nodes and pathrater is used to avoid the packets to route through the misbehaving path. This protocol require bidirectional communication for reliable transmission.[21]

3.3 Trusted GPSR

The Greedy Perimeter Stateless Routing [22] is modified to take trust levels of node into account. Each time a node transmits a packet it waits until it overhears its neighbouring node forwarding it. Based on the accurate and timely forwarding actions, it maintains a trust value for its neighbours. This information is then taken into account for further routing decisions.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

3.4 Trust based Routing Protocol (TRANS)

As it was proposed in [19] the TRANS protocol develops a trust relationship between the source node and the sink node. It uses asymmetrical authentication for trust routing and provides a trusted path that denies malicious nodes to enter the network. It has been assumed that sensors know their location and neighbouring nodes by geographic routing and shared encryption key is applied to authenticate the messages that reach the sink node or base stations in order to achieve confidentiality. The sink node sends its message only through trusted neighbours.

3.5 Cluster Based Trust aware Routing Protocol (CBTRP)

In [23] it has been proposed that the forwarding packets are protected from malicious nodes in a clustered environment where the cluster head is elected which is in one hop distance from the base station. The packets are forwarded only through trusted nodes based on the trust metrics. The trust metrics between nodes are developed based on the time and frequency interactions. The packets are forwarded only through trusted cluster heads and as in case if cluster head becomes malicious another trust worthy neighbour cluster header is elected.

3.6 Trust Aware Routing Protocol (TARP)

Without taking time synchronization and geographic information into account the TARF provides a trust worthy and energy efficient routing of nodes in the network. As suggested in [24] it has been proposed that TARF proves to be effective against various attacks like sinkhole attack, worm hole attacks and Sybil attacks. It also proves that TARF provides the effective way of nodes to avoid replaying of routing information.

3.7 Ambient Trust Sensor Routing (ATSR)

In [5] it has been proposed about the working model of ATSR. In this approach, nodes observe the performance of their neighbours with respect to different trust metrics and obtain the direct trust value per neighbour. It also, takes into account indirect trust information, i.e. trust information from its neighbours, which is called as reputation. Direct and in- direct trust information is collective used to reach the total Trust information. Finally, the routing decisions are based on two parameters i.e. geographical information (distance to the base-station) and Total Trust information. The trust model presented has been integrated with a location-based routing protocol .If no malicious node exists in the network, i.e. the Total Trust is almost equal to 1, the ATSR behaves simply the Greedy Perimeter Stateless Routing (GPSR) protocol.

IV TRUST MODELS

According to reference [17] the methods for obtaining trust information and defining each node's trust worthiness are referred to as a trust model. Trust models are used in cluster head election and key distribution in order to improve security and increase throughput, lifetime and flexibility of a sensor network. Wireless sensor networks are mainly deployed to monitor events and report data, both continuous and discrete which leads to the growth of new trust models addressing the permanent data issue and also to combine the data trust and the communication trust to infer the total trust.[21]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

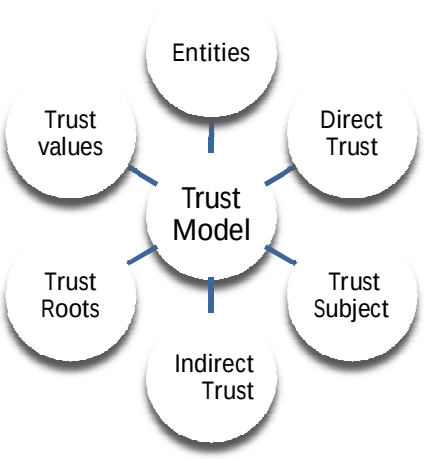

Fig 1. Trust Management Model for WSN.

Entities are the subject objects of trust relationships. Trust roots are called as seeds of trust, where the positive assumptions about the specific entities are made by all entities in the same community [17]. The nodes monitor the behaviour of their neighbours that are within the communication range and based on the trust metrics they calculate the direct trust and indirect trust and generates various trust values for their corresponding neighbours.

Many network models have been proposed in recent years and many researchers have concentrated on various trust management schemes. It has been assumed that each cluster nodes are stationary and the physical location and communication range in the network are known. The clusters of sensors can be formed based on various criteria such as capabilities, location and communication range [25]. An accurate trust model should be build among the nodes in order to protect the nodes from various so called attacks like denial of service attacks, sink hole attacks, black hole attacks etc. Various trust metrics have to be considered and trust values are calculated among nodes and even for cluster heads in order to build a trusty relationship between the communicating nodes.

V FUTURE WORK AND CONCLUSION

In this paper it has been studied about various attacks that arise in a clustered based wireless environment and also we discussed about the various trust management routing protocols that are available for secure routing. As many algorithms have been proposed for providing trust among nodes and various efficient solutions have been given for various attacks still there are few problems have to be addressed in clustered situations in case of denial of service attacks between the clustered networks towards the base station in a heterogeneous environment. So as a future work we can concentrate towards the heterogeneous cluster based trust aware routing to provide a efficient and secure data communication between the nodes and the base station.

REFERENCES

[1] John A. Stankovic, *Wireless Sensor Networks* University of Virginia, Charlottesville, Virginia 22904.

[2] Adhoc Wireless Networks, Architectures and protocols by C.Siva Ram Murthy and B.S.Manoj

[3] C.Karlof and D.Wagner, "Secure Routing in wireless sensor networks: attacks and countermeasures," in *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, 2003.

[4] M.Jain and H.Kandwal, "A survey on complex wormhole attack in wireless and ad hoc networks," in *Proceedings of International Conference on Advances in Computing, Control , and Telecommunication Technologies* (ACT '09), 28-29 2009, pp. 555-558.

[5] I.Krontiris, T.Giannetsos, and T.Dimitriou, "Launching a sink-hole attack in wireless sensoe networks: the intruder side," in *Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications(WIMOB '08)*, 12-14 2008, pp. 526-531.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[6] J.Newsome, E.Shi, D.Song, and A.Perrig, "The sybil attack in sensor network: Analysis and defenses," in *Proceedings of the 3rd International Conference on Information Processing in Sensor Networks(IPSN'04)*, Apr. 2004.

[7] Tim Daniel Hollerung, University of Paderborn, "The Cluster-Based Routing Protocol", Project Group 'Mobile Ad-Hoc Networks based on Wireless LAN'

[8] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and countermeasures", University of California at Berkeley.

[9] Emmanuel Bresson, Mark Manulis, "Contributory Group Key Exchange in the Presence of Malicious Participants", in *Proceedings of IET Information Security(IET-IFS)*, Vol 2, Issue 3, pp. 85-93, September 2008.

[10] Mark Manulis, "Provably Secure Group Key Exchange", *Disertation* for the *Degree of Doktor-Ingenieur*, Dept of EE&IT(Germany); Network & Data Security(NDS) group.

[11] Vivek Mhatre, Catherine Rosenberg, "Homogenous Vs Heterogeneous Clustered Sensor Networks: A Comparative Study", School of Electrical and Computer Engineering, Purdue University, West Lafayelte, IN 4790-1285.

[12] V.Mhatre, C.Rosenberg, "Design Guidelines for Wireless Sensor Networks: Communication, Clustering and Aggregation", in the *Proceedings of Adhoc Networks Journal*, Elsevier Science.

[13] 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" in the *Proceedings of International Journal of Network Security & Its Applications (IJNSA)*, Vol.2, No.3, July 2010

[14] Ms. Dipali Dikondwar, R. K. Krishna, "Survey : Energy-Efficient and Trust-Aware Routing Techniques for WSN", in the *Proceedings of the International Journal of Engineering Research & Technology (IJERT)*, ISSN: 2278-0181, Vol. 2 Issue 2, February- 2013.

[15] Guoxing Zhan, Weisong Shi, Julia Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs", in the *Proceedings of IEEE TRANSACTIONS on DEPENDABLE AND SECURE COMPUTING.*

[16] Vinay Sony, Pratik Modi, Vishvash Chaudhri, "Detecting Sinkhole Attack in Wireless Sensor Network" *Internationl journal of application or Innovation in Engineering & Management, volume 2, issue 2, Febuary 2013.*

[17] Theodore Zahariadis, Helen Leligou, Panagiotis Karkazis, Panagiotis Trakadas and Stamatis Voliotis "Trust Management in Wireless Sensor Networks " *EUROPEAN TRANSACTIONS ON TELECOMMUNICATIONS, Eur.Trans, telecoms,2010;21:386-395.Published online 8 April 2010 in Wiley InterScience.*

[18] A Trusted AODV Routing protocol for Mobile Adhoc Networks.

[19] Secure IsolatingCompromised Sensors in Location-Aware Sensor Networks *Sapon Tanachaiwiwat1, Pinalkumar Dave1, Rohan Bhindwale2, Ahmed Helmy11. Department of Electrical Engineering – Systems 2. Department of Computer ScienceUniversity of Southern California, Los Angeles, CA. 900891 (213) 740 9135{tanachai, pdave, bhindwal, helmy} @usc.edu*

[20] Adhoc Wireless Networks *architectures and protocols by C.Siva Ram Murthy and B.S.Mano published by pearson education.*

[21] *Survey of trust Models in Different Network DomainsMohammad Momani ,Subhash Challa , Faculty of Engineering and Information Technology, UTS, Sydney, Australia, NICTA, VRL, University of Melbourne, Australia*

[22] A. A. Pirzada and C. McDonald, "Trusted Greedy Perimeter Stateless Routing," *Proceedings of the* 15th *International Conference on Networks*, Adelaide, 19-21 November 2007, pp. 19-21. doi:10.1109/ICON.2007.4444087

[23] A cluster-based trust-aware routing protocol for mobile adhoc Networks, *Haidar Safa Æ Hassan Artail Æ Diana Tabet,* Wireless Netw DOI 10.1007/s11276-009-0182-1

[24] T. Zahariadis, H. C. Leligou, P. Trakadas and Stamatis Voliotis, "Mobile Networks Trust Management in Wireless Sensor Networks," *European Transactions o Telecommunications*, Vol. 21, No. 4, 2010, pp.386-395.

[25] Junqi Zhang, Rajan Shankaran, Mehmet A. Orgun, Vijay Varadharajan "A Trust Management Architecture for Hierarchical Wireless Sensor Networks" Department of Computing, Macquarie University, Sydney, Australia