International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:2, 2014

Review of Trust Models in Wireless Sensor Networks

V. Uma Rani, K. Soma Sundaram

***Abstract*—**The major challenge faced by wireless sensor networks is security. Because of dynamic and collaborative nature of sensor networks the connected sensor devices makes the network unusable. To solve this issue, a trust model is required to find malicious, selfish and compromised insiders by evaluating trust worthiness sensors from the network. It supports the decision making processes in wireless sensor networks such as pre key-distribution, cluster head selection, data aggregation, routing and self reconfiguration of sensor nodes. This paper discussed the kinds of trust model, trust metrics used to address attacks by monitoring certain behavior of network. It describes the major design issues and their countermeasures of building trust model. It also discusses existing trust models used in various decision making process of wireless sensor networks.

***Keywords*—**Attacks, Security, Trust, Trust model, Wireless sensor network.

I. Introduction

WIRELESS SENSOR NETWORKS contains thousands of sensor nodes with less memory and low power devices. It is vulnerable to insider and outsider attacks because of collaborative and dynamic nature. Several cryptographic algorithms were available for generic enhanced securities, but most of them are not suitable for wireless sensor networks. Cryptography mechanism does not enough to prevent any insider attacks, because those algorithms could not identify malicious node or selfish behavior of nodes. But it does not provide additional security or no explicit rules to protect each node and also no enhancement of distributed data gathering and collaborative data processing in networks. The main purpose of the trust model is to enhance the overall performance by monitoring network activities, minimizing the risk and ensuring the network activities of entity such as data gathering and data processing.

The term trust management was introduced by Blaze et al. [4] to define a coherent framework for the study of security policies, credentials and trust relationships. The term trust has been defined by several ways, as The Merriam-Webster's Dictionary [2] defines trust as "assured reliance on the character, ability, strength, truth of someone or something".

Dictionary.com [2] describes trust as the "firm reliance on the integrity, ability or character of a person or thing". In brief, trust is the reputation of entity [44] where reputation is opinion about others. Trust is a belief [45] that ensures entity as secure and reliable. Thus trust model is used to differentiate trust worthy and untrustworthy nodes in a network. It encourages trustworthy nodes to communicate and discourages untrustworthy nodes to participate in the network. Also, it increases the network lifetime, throughput and resilience of the wireless sensor network.

In this paper the sections are organized as follows: Section II deals with kinds of trust model, Section III discusses most widely used trust metrics and attacks addressed, Section IV discusses the major design issues and their countermeasures in trust model, Section V reviews various trust models discussed in the literatures.

II. Kinds of Trust Model

In wireless sensor network, trust specifies the reliability or trust worthiness of sensor node. Trust [3] may be classified in different ways based on how they are used. Trust may be subjective or objective based on task. Depending on property, trust may be social trust or QOS trust. Social trust considers intimacy, honesty, privacy, centrality, connectivity and QOS trust considers energy, unselfishness, competence, cooperativeness, reliability, task completion capability, etc. In general, trust may be classified as behavioral or computational trust based on where it is used. Behavioral trust defines trust relations among people and organizations. Computational trust defines trust relation among devices, computers, and networks.

Depending on the observation, trust may be direct trust or indirect trust. Direct trust specifies the direct observations and called as first hand information. Indirect trust specifies the indirect observation and called as second hand information. The trust values calculated between nodes are based on their cooperation in routing messages to other nodes in the network which is termed as communication trust. The trust value calculated is based on the actual sensed data of the sensors in wireless sensor networks is known as data trust.

In wireless sensor networks, trust model specifies plays an important role in identifying misbehavior nodes and providing collaboration among trustworthy nodes. It improves the lifetime of networks that inspire expectations among future interactions. The model is capable of capturing and distributing feedbacks about current interactions among nodes and stores the trust information for future. It also uses feedback to guide trust decisions. Depending on trust information stored, it may be classified as centralized, distributed and hybrid Model [1] and given in Fig. 1.

V.Uma Rani is with the Computer Science and Engineering Department in Jaya Engineering College, Tamil Nadu, India (Phone:91-978-999-6578, e-mail: umaranibharathy@gmail.com).

Dr. K. Soma Sundaram is with the Computer Science and Engineering Department in Jaya Engineering College, Tamil Nadu, India (Phone: 91-962-921-5196, e-mail: soms79@gmail.com).

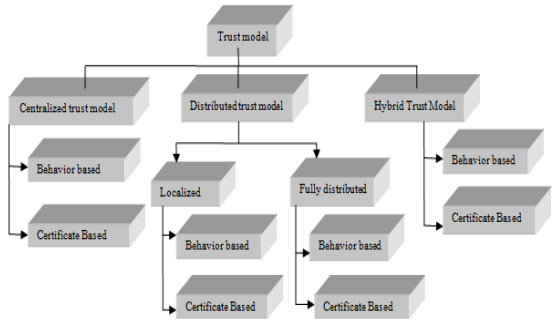

Fig. 1 Kinds of Trust model

Centralized trust model consists of a single globally trusted server that determines the trust values of every node in the network. In distributed trust model, every node locally calculates the trust values of all other nodes in the network that increases the computational cost. Also each node needs to maintain an up-to-date record about the trust values of the entire networking in the form of a table.

Hybrid trust model contains the properties of both centralized as well as distributed trust management approaches. The main objective of this approach is to reduce the cost associated with trust evaluation as compared to distributed approaches. This scheme is used with clustering schemes in which cluster head acts as a central server for that cluster. The main advantages and disadvantages of trust model are listed in Table I.

TABLE I
PROS AND CONS OF TRUST MODEL

Structure	Pros	Cons
Centralized	Least computational overhead, least memory usage	Most Communication overhead, least reliable, lack of scalability
Distributed	Most reliable and scalable	Most computational overhead
Hybrid	Less communication overhead than centralized and less memory	Large computational overhead than centralized, large memory requirement than centralized , less reliable and scalable compared to distributed

In the certificate-based trust model, trust is mainly based on the provision of a valid certificate assigned to a target node by a centralized certification authority or by other trusted issuer. In the behavior-based trust model, an entity calculates the trust values by continuous direct or indirect monitoring of other nodes.

III. TRUST METRICS AND ATTACKS ADDRESSED

There are several trust metrics taken by trust model to calculate the trust value. Trust metric is a measure of how a member of one group is trusted by other. Trust metric may be classified as deterministic or probabilistic, binary, discrete or continuous and symmetric or asymmetric. Table II discusses some of the trust metric [2] monitored by trust models and the attack addressed by corresponding trust metric.

TABLE II
TRUST METRICS, MONITORED BEHAVIOR AND ATTACKS ADDRESSED

Trust metric	Monitored behavior	Attacks addressed
Data Packets forwarded	Data message / packet forwarding	Black hole, sink hole, selective forwarding
Control packets forwarded	Control message forwarding	Control/Routing message dropping
Data packet /Message precision	Data integrity	Data message modification
Control packet /Message precision	Control packet integrity	Sybil attack and any attack based on routing protocol message modification
Availability based on beacon/hello messages	Timely transmission of periodic routing information reporting link/node availability	Passive eavesdropping, selfish node, Hello flood attack
Network layer Acknowledgement	To check successful transmission of message	End to End forwarding, Colluding adversaries.
Packet address modified	Address of forwarded packets	Sybil, Wormhole
Cryptography	Capability to perform encryption	Authentication attacks, Sniffing attack
Routing protocol execution	Routing information	Misbehaviors related to specific routing protocol actions
Battery life time	Remaining power sources	Node availability and Position, traffic analysis attack
Consistency of reported values /data	Consistency of sensing results, reported values	Compromised nodes, No response attack
Sensing communication	Reporting of events	Selfish node behavior at application level
Reputation validation	Trust value obtained from third parties	Bad mouthing attack, Fake Warning-report attack
Hop Count scheme	Number of nodes forward request	Lying about hop count, Sybil attack
Reputation Response	Check the execution of reputation mechanism	Selfish node attack

IV. TRUST MODEL DESIGN ISSUES AND COUNTERMEASURES

Trust model can be designed by considering the three major components such as Information gathering, information modeling, information dissemination, spurious rating, detection and response. Each stage has several issues that can be considered carefully in design of trust model in Wireless sensor networks [2], [47].

A. Information Gathering

Information gathering is a process in which, a node collects information about other nodes that is interested. In general, Information can be obtained by manually (feedback) or automatic sources. In wireless sensor network, Information may be gathered as direct observation (first hand information) or indirect observation that is second hand information (called

reputation).Second hand information can be collected by propagating information through nodes which are vulnerable to bad mouthing attack and ballot Attack. In bad mouthing attack, attackers give negative feedback about well behaved nodes to decrease the trustworthiness. In ballot attack, malicious node gives positive feedback to other malicious nodes to increase their trustworthiness.

B. Information Modeling

It specifies how node calculates reputation value of other nodes which are participating in the networks. Reputation value can be calculated using deterministic or probabilistic approaches. In centralized approach, reputation value is calculated by deterministic approaches. In distributed approach, each node calculates reputation values itself using probabilistic approaches. Hybrid approach is combination of centralized and distributed approach. So it uses probabilistic or deterministic approaches.

C. Information Dissemination

Information sharing involves three important issues: (i) dissemination frequency, (ii) dissemination locality, and (iii) dissemination content. Dissemination frequency may be proactive (share information at each interval specified) or reactive (share information when any accepted changes). Dissemination locality may be local (information published within a neighborhood node) or global (the information is propagated to nodes outside the radio range of the node publishing the reputation information).The content is raw information or processed information that shares false reporting attack. Information can be disseminated by centralized or distributed way depending on the structure.

D.Redemption, Spurious Rating and Weighting of Time

An important issue in maintaining and updating reputation is how past and current information are weighted. Generally first hand observation has more weight than second hand information. If second-hand information is used to influence reputation, some nodes may lie and give spurious rating about others.

E. Detection and Response

It specifies how to detect misbehaviors and specify the response of system. Here, uses several trust metrics to calculate trust value that can be used to find misbehaviors. Response may give punishment or reward that also one of the issues in trust management system. Each and every stages of designing trust model provide additional security vulnerabilities and has several solutions [20] for careful design of trust model as in Table III.

V. Existing Trust Models

Trust plays an important role in human life environments and virtual organizations. Trust is an important issue in distributed system [10], [43]. In e-services, trust estimate the risk of transaction involved between buyers and sellers. For example policy maker and key note as first trust management used in web services. Amazon, eBay, and NetFlix [5], have deployed reputation-based trust in ranking their products and suppliers. In the context of a network, trust may help its elements to decide whether another member of the same network is being uncooperative or malicious. In Ad-hoc network, trust plays an important role in finding misbehaviors, routing, cooperation and resource sharing. Trusted AODV [23], Trusted GPSR [24], Trust Aware DSR [25] and CONFIDENT [21] are responsible for routing. CORE [22], OCEAN [40] are responsible for cooperation among nodes in Ad-hoc Network.

In wireless sensor network, trust plays a major role in detecting a node which is not behaving as expected (either faulty or maliciously). Trust judges the quality of node and their services. Also it assists on decision making process such as data aggregation, routing and reconfiguring sensor nodes. This paper focuses mainly on various trust models used in wireless sensor network.

The reputation-based framework for high integrity sensor network (RFSN) [6] is a first trust based model designed and developed for sensor networks. It makes use of watchdog mechanism to collect data and monitor different events in the node to build reputation of the node and then get the trust rating of the node. Some of the proposed improved models of beta based reputation in sensor networks are MA&TP-BRSN [7], RFM-WSN [8]. The RASN [39] is reputation agent based framework for WSN to incorporate on/off attack resisting model which is improved model of RFSN.

TABLE III
Design Issues, Vulnerabilities and Defense Mechanism Used

Design issues	Additional security vulnerabilities /attacks	Defense mechanism used
Direct information gathering	False behavior, collusion, intentional collision/ limited overhearing and partial dropping.	Neighbor based monitoring; acknowledgement based monitoring, indirect observation.
Indirect information gathering	Unreliable information / false behavior attack, conflict behavior attack, ballot attack, badmouthing attack.	Anomaly detection, eliminate unwanted information and redundancy.
Information dissemination	False reporting attack, on/off attack, Denial of Service attack.	Proactive /re active dissemination approach.
Redemption, Spurious Rating and Weighting	False positive /false negative attack, drop packet attack., slandering attack	Authentication key, Monitor the behavior of sleep and wake up nodes, Give proper weight for direct observation than indirect observation, dynamic redemption approach.
Detection and response	Incomplete trust threshold, new comer or identity or white washing attack, miss detection and false alarm.	Optimized trust threshold, dynamic trust threshold.

The watchdog is responsible for detecting non forwarding behavior of node in a network. Extended watchdog [11] mechanism is used to monitor all its neighbors' behavior based on information collected from MAC layer. It uses new direct last-hop neighbor behavior evaluation mechanism (LHDA) which collects information from MAC layer when RTS/CTS/DATA/ACK control packets are enabled. It is mainly based on direct observations and it has low computation overhead and resilience to attacks.

The Retrust [34] is an attack-resistant and lightweight trust management scheme to detect faulty or malicious behaviors and improve the performance of medical sensor network. The Bayesian fuse algorithm [33] used to combine more than one trust component to evaluate trust worthiness of all nodes in a network. It uses communication trust (beta distribution) and data trust for trust calculation. It reduces the false reporting attack.

The LDTS [35] is a lightweight and dependable trust system for clustered wireless sensor networks which uses direct trust and feedback trust to improve decision making and collaborative processing by detecting malicious behaviors. The hierarchical trust management for wireless sensor networks (HTMW) [36] performs multi path routing when intrusion detected in wireless sensor network. It evaluates the trust worthiness of node using subjective trust (performance at running time) and objective trust (node status). Also it uses QOS trust as well as Social trust to evaluate the trust worthiness of node.

The agent-based trust model for Wireless Sensor Networks (ATSN) and Agent based Trust management (ATRM) [9] are agent based reputation approaches. In ATRM, distributed certificate based trust model monitor the behavior of network with the help of agent module. Agent module performs the reputation calculation by issuing t-certificate. Sensor node decides the transaction of node or not from mobile agent by issuing r-certificate. It addresses the uncertainty issue, but still cooperates with the malicious nodes and has one value of trust rating for different events.

The bio-inspired trust and reputation model, called BTRM-WSN [12**]** is a distributed based ant colony approach which is used to improve the collaboration among nodes by selecting most trustworthy nodes along the path from sensor node to sink node. The quality based distance vector QDV [13] is an ant colony based reputation model used to provide reliable communication and to provide QOS based security in WSN. It protects the network from packet injection attack. Both [12], [13] are based on ant colony reputation based approach which has less scalability and new benevolent user has good chance of selection as a new service provider. The TMA [31] is dynamic certification based trust management architecture for hierarchical WSN that reduces the computation and communication overhead by considering both behavioral and direct trust.

The reliable data aggregation and transmission protocol, called RDAT [14] is a distributed functional based beta reputation model. It improves the reliability of data aggregation and transmission by evaluating each type of sensor node action using a respective functional reputation. It prevents false injection attack /compromised attack. The trust-based secure data aggregation protocol (TBS) [27] used to select the aggregator which has highest combined trust value to avoid aggregation attacks. The robust adaptive approach based on hierarchical monitoring (RAHIM) [28] is a centralized reputation scheme which provides secure data aggregation and less communication overhead in cluster based wireless sensor networks. The reputation-based secure data aggregation (RSDA) [32] is used to improve the accuracy of aggregated data and enhance the network lifetime.

The trust management model for internet of things called TRM-IoT [15] is a fuzzy based reputation model which is used to establish collaboration among nodes and to monitor malicious misbehavior. The trust model use fuzzy logic [30] which is used to provide efficient and safe communication from source to destination.

The Sensor Trust [17] is a resilient model for improving data integrity. It evaluates the trust worthiness of node in hierarchical WSN using Gaussian distribution-based fine-grained method. The Ambient Trust Sensor Routing (ATSR) [18] is a trust-aware, location-based routing protocol which protects the WSN against routing attacks, and also supports large-scale WSNs deployments. It is used to evaluate the reliability of the nodes by weighted reputation mechanism. The addition encouragement and multiplication punishment (AEMP) [19] is a new routing trust based protocol to enhance ability against attacks from inside network. It needs more computation and communication resources to decide best route. The direct trust dependent link state routing protocol (DTLSRP) [26] is a trust based routing protocol to protect network from routing attacks. The role based trust management language (RT) [16] is used for representing security policies and credentials in decentralized, distributed access control systems. For example Policy maker, Keynote, SPKI/SDSI, Role Based Access control (RBAC) are based on RT language and RT^D specify policies over wireless sensor node which delegates their roles to other node when location changes. It specifies delegation based on attributes not their identities.

The RRAS [46] is the reputation based role assignment method for assigning roles or levels of node to improve throughput of wireless sensor network. The distributed reputation based beacon trust system (DRBTS) [37] is a reputation based distributed structure for monitoring misbehaviors of WSN. It is a first reputation model for secure localization using voting majority scheme.

The resilient geographic routing protocol (RGR) [29] is used to provide secure, validated localization and trust based routing using probabilistic multi path routing protocol. It prevents broadcast manipulation attack such as mobility attack, multiple unicast packet attack and byzantine attacks.

The TMF [38] is a dynamic trust management framework which reduces communication overhead, computation overhead and memory requirements by combining both behavior and certificate based scheme.

Table IV shows several techniques to build a trust model in sensor networks with their purpose, architecture used, type of reputation calculation and so on. Trust model plays several roles in wireless sensor network [6]-[9], [11] focused on monitoring, detect malicious behaviors, [12], [13], [15], [18] improve collaboration among sensor nodes, provide reliable communication, [18], [19], [21], [23] and [24]-[26], [36], [41] focuses reliable routing, provide secure localization[29], [37], provide access control [16], [46] and [14], [27], [28], [32] improve aggregation among sensor nodes. The works presented [6]-[8], [11]-[13], [15], [18], [19], [30], [33]-[35] has focused on communication behavior for predicting trust worthiness of nodes. But [14] focused on trust to improve data integrity which is important for data aggregation in network.

TABLE IV
DESIGN OF EXISTING TRUST MODELS IN WIRELESS SENSOR NETWORKS

Trust Model	Structure	Information modeling	Information gathering	Information propagation	Information dissemination	Redemption	Simulator / tool used	Detection and Response
RFSN[6]	Distributed and cooperative	Beta distribution approach	Reputation	Self to neighbor and neighbor to neighbor	yes	yes	TRM Sim –WSN	Selfish /malicious routing, packet forwarding
ATRM [9]	Hierarchical, Certificate based	Agent based	Reputation	MN to SN,SN to MN	Optimal threshold	no	NS2	Misbehavior attack
DRBTS [37]	Distributed and cooperative	Quorum voting approach	Reputation	Self to neighbor and neighbor to neighbor	BN to SN ,BN to BN	yes	JSIM	Selfish /malicious routing and packet forwarding
AEMP [19]	Distributed	Weighted approach	Reputation	BN to SN	BN to SN	yes	Mat lab	Selfish /malicious routing
RDAT [14]	Distributed	Beta distribution	Functional Reputation	Self to neighbor and BN to SN	false positive to neighbor	no	TOSSIM	False injection /compromised attack
TRM-IoT [15]	Distributed and behavior based	Fuzzy	Reputation	Self to neighbor	SN to SN	no	NS3	Selfish /malicious routing
BTRM [12]	Distributed	Ant Colony	Reputation	Self to neighbor, neighbor to neighbor	SN to ant ,ant to SN	yes	TRMSim-WSN	Malicious misbehavior
DTLSRP [26]	Distributed	Weighted	Direct trust	SN to neighbor, Neighbor to SN	yes	No	Mat lab	Routing attacks
TMA [31]	Behavior and Certificate based Hierarchical	Weight based	Reputation	SN to CH ,CH to CH,CH to SN	Integer number from 1-100	no	NS2	Malicious packet forwarding
RSDA [32]	Distributed	Beta probability	Reputation	SN to SN, SN to BN	positive or negative to SN	no	NS2	Malicious/packet forwarding mis-behavior, replay attack
LDTS [35]	Hierarchical	Weight based Approach	Reputation based	CH-to-CH, BS-to-CH, CM to CM,CH to CM	Optimal trust threshold	no	Net-Logo based trust engine	Malicious misbehavior
HTMW [36]	Hierarchical	Stochastic Petri net	Reputation based	SN to SN, CN to SN, Peer to Peer , CH to CH	Optimal trust threshold	no	NS2	malicious behaviors and routing attacks
RESRP [42]	Hierarchical	Redemption based weight	Reputation based	BN to SN, SN to neighbors	Redemption factor	no	-	Selective forwarding, Sybil attack, Wormhole attack, On/Off attack

[a]CH-cluster head BS-Base Station, SN-Sensor node MN-Mobile Node, CM- Cluster Member

Some research works [11] are mainly based on direct observations or subjective observation which does not enhance the functionality and not observed all kinds of attacks in wireless sensor network.

In each research work, authors use different mechanism or reputation calculation such as beta distribution [6]-[8]. and [14], [32], [46], weighted approach [17], [26], [27], [31] and [35], [38], [42], Bayesian approach [21], [22], [33] ant colony approach [12], [13], fuzzy [15], [30], agent based [9], [39] and so on. Work [6]-[8], [14], [32], [46] are mainly based on beta based reputation model which is effective approach to monitor network behavior, give reward and punishment based on their behavior of forwarding packets, but not focused on functional based or event based sensor nodes. It does not differentiate positive or negative events in sensor network. In weight based approach [17], [26], [27], [31], [35], [38], [42] trust worthy node is selected based on how they are weighted and trust node is capable to compare received data with sensed data duration and is mainly based on synchronization. In agent based approach [9], [39] agent node is responsible for trust calculation. So, Agent node has long radio range, more power and large storage base. Beacon trust model which uses reputation values that is vulnerable to attacks. There is no general trust model suitable for all kinds of application in wireless sensor network and previous research work focused on derivation of new trust relations from old ones; e.g., trusted third-party services, transitive trust relations, delegation. Now, researchers are focusing on how to create new trust relations that are not derived from old ones, and create new opportunities for cooperation among users and among services.

VI. CONCLUSION

The need of trust model in wireless sensor network is

extensively discussed in this paper. Trust metrics, issues in building a wireless sensor networks and some of the research work done on trust management are also discussed. There is no standard adversarial model where current trust systems compete to provide a higher level of security or resilience to attacks. The designers of each system solved the trustworthiness problem in WSNs from different angles and some designers solved the problem by considering only routing misbehaviors or only depend on task and so on.

It is believed that each activity, such as routing or data aggregation has its own challenges and need to be considered carefully. Trust model in wireless sensor network cause new attacks such as ballot attack, bad mouthing attack, selective behavior attack, on-off attack, new comer attack and so on. So the researchers developed a trust model carefully to handle wireless sensor network attack as well as trust attacks. Future research work in trust management focuses on generalized, scalable and reconfigurable trust model suitable for distributed computing system. It handles malicious and non malicious misbehavior in networking, sensing and data processing. This can improve the security issues to meet specific application demands.

REFERENCES

[1] Huaizhi Li and Mukesh Singhal, "Trust Management in distributed Systems", *IEEE Computer Society*, pp: 45-53, 2007.

[2] Vishal Rathod, Mrudang Mehta, "Security in Wireless Sensor Network", *A survey in Journal of Engineering & Technology*, Vol.-1, Issue-1, pp.35-45, 2011.

[3] Theodore Zahariadis, Helen C. Leligou, Panagiotis Trakadas and Stamatis Voliotis, "Mobile Networks- Trust management in wireless sensor networks" *in European Transactions on Telecommunications*, pp. 386–395, 2010.

[4] M.Blaze, J.Feigenbaum, and J.Lacy,"Decentralized Trust Management" *in IEEE Symposium on Security and Privacy*, pp.150-168, 1996.

[5] Ling Liu, Weisong Shi," Trust and Reputation management" *in IEEE Internet Computing*, pp.1089-7801, 2010.

[6] S. Ganeriwal, L. K. Balzano, M. B. Srivastava, "Reputation-based framework for high integrity sensor networks" *in ACM Transactions on Sensor Networks* pp.1-37, 2008.

[7] Yang Guang, Yin Gui-sheng, Yang Wu et al, "Reputation Model based on behavior of sensor nodes in WSN", *in Journal on Communication*, pp. 18-26, 2009.

[8] Xiao De-qin, Feng Jian-zhao, Yang Bo et al," Reputation formal model for wireless sensor network" *in Computer Science*, pp.84-87,2007.

[9] Boukerch , L. Xu , K. EL-Khatib,"Trust-based security for wireless ad hoc and sensor networks" *in Computer Communications*, pp. 2413–2427,2007.

[10] Li Lin and Jinpeng Huai, "QGrid: An Adaptive Trust Aware Resource Management Framework", in *IEEE Systems Journal*, Vol. 3, No. 1, pp. 78-90, 2007.

[11] Lei Huang , Lixiang Liu, "Extended Watchdog Mechanism for Wireless Sensor Networks" *in Journal of Information and Computing Science* Vol.3, No. 1, pp. 39-48,2008.

[12] Félix Gómez Mármol, Gregorio Martínez Pérez, "Providing trust in wireless sensor networks uses a bio-inspired technique" *in Journal on communication*, pp.86-94, 2008.

[13] S.K. Dhurandher, S. Misra, M.S. Obaidat, N. Gupta, "An ant colony optimization approach for reputation and quality-of-service-based security in wireless sensor networks" *in Security and Communication Networks*, pp. 215–224,2009.

[14] Suat Ozdemir, "Functional reputation based reliable data aggregation and transmission for wireless sensor networks" *in Computer Communications* pp 3941–3953, 2008.

[15] Dong Chen, Guiran Chang, Dawei Sun, Jiajia Li, Jie Jia, and Xingwei Wang," TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things" *in ComSIS Vol. 8, No. 4, Special Issue*, pp. 1208-1228. 2011.

[16] Anna Felkner, "How the Role-Based Trust Management Can Be Applied to Wireless Sensor Networks" *in journal of telecommunications and information technology*, pp. 70 -78, 2011.

[17] Guoxing Zhana, Weisong Shi, Julia Deng, "SensorTrust: A resilient trust model for wireless sensing systems"*in Pervasive and Mobile Computing*, pp.509–522, 2011.

[18] 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 WSN" *in International Journal Of Network Security & Its Applications* (IJNSA), Vol.2, No.3,pp.123-143,2010.

[19] Gu Xiang, Qiu Jianlina, Wang Jina, "Research on Trust Model of Sensor Nodes in WSNs" ,*in International Workshop on Information and Electronics Engineering (IWIEE)*, pp.45-57,2012.

[20] Youngho Cho and Gang Qu, Yuanming Wu, "Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks" *in IEEE Symposium on Security and Privacy Workshops*, pp. 134-141,2012.

[21] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the CONFIDANT protocol (Cooperation Of Nodes- Fairness In Dynamic Ad-hoc NeTworks)", *in The 3rd ACM Internationa symposium Mobile Ad-hoc Networking & Computing (MobiHoc '02)*, Lausanne, CH, 2002

[22] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad-hoc Networks" *in The IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security* Portoroz, Slovenia, 2002.

[23] X. Q. Li, M. R. Lyu and J. C. Liu, "A Trust Model Based Routing Protocol for Secure Ad-Hoc Networks" *in Proceedings of the IEEE Conference on Aerospace, Big Sky,Montana*, Vol. 2, 6-13 March 2004.

[24] A. A. Pirzada and C. McDonald, "Trusted Greedy Perimeter Stateless Routing *in Proceedings of the 15th IEEE International Conference on Networks*", *Adelaide*, November, pp. 19-21,2007.

[25] S. Marti, T. Giuli, K. Lai and M. Baker,"Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks*"in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, ACM Press, Boston,(6-11), pp. 255-265,2000.

[26] Shaik Sahil Babu, Arnab Raha, Mrinal Kanti Naskar ,"A Direct Trust Dependent Link State Routing Protocol Using Route Trusts for WSNs (DTLSRP)" *in Journal of Scientific Research Wireless Sensor Network*, 3,pp 125-134,2010.

[27] Bhavna Arora Makin and Dev Anand Padha,"A Trust-Based Secure Data Aggregation Protocol for Wireless Sensor Networks" *in IUP Journal of Information Technology*, Vol. VI, No. 3,pp 7 – 22,2010.

[28] Nabila Labraoui,Mourad Gueroui,Makhlouf Aliouat,Jonathan Petit, "RAHIM: Robust Adaptive Approach Based on Hierarchical Monitoring Providing Trust Aggregation for Wireless Sensor Networks" *in Journal of Universal Computer Science*, vol. 17, no. 11 , 1550-1571,2011.

[29] Ke Liu, Nael Abu-Ghazaleh , Kyoung-Don Kang, "Location verification and trust management for resilient geographic routing" *in Journal of Parallel and Distributed Computing*, 67,215 – 228,2007.

[30] Tae Kyung Kim, and Hee Suk Seo ,"A Trust Model using Fuzzy Logic in Wireless Sensor Network"*in World Academy of Science, Engineering and Technology*, 18, pp 61-66,2008.

[31] Junqi Zhang, Rajan Shankaran, Mehmet A. Orgun Vijay Varadharajan and Abdul Sattar ,"A Trust Management Architecture for Hierarchical Wireless Sensor Networks" ,*35th annual IEEE conference on local computer networks.LCN* ,pp. 268-273,2010.

[32] Alzaid, Hani and Foo, Ernest and Gonzalez Nieto,"RSDA: Reputation-based Secure Data Aggregation in Wireless Sensor Networks"*in Proceedings 1st International Workshop on Sensor Networks and Ambient Intelligence* (SeNAmI), Dunedin, New Zealand, 2008.

[33] Mohammad Momani,"Bayesian Fusion Algorithm for Inferring Trust in Wireless Sensor Networks" *in Journal of networks*,vol.5,no.7,pp.815-824,2010.

[34] Daojing He, Chun Chen, Sammy Chan, Jiajun Bu, and Athanasios V. Vasilakos, "ReTrust: Attack-Resistant and Lightweight Trust Management for Medical Sensor Networks" *in IEEE transactions on information technology in biomedicine*, vol. 16, no. 4, pp.623-632, 2012.

[35] Xiaoyong Li, Feng Zhou and Junping Du,"LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks" *in IEEE transactions on information forensics and security*,pp451-551, 2013.

[36] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection" *in IEEE Transactions on network and service management*, vol. 9, no. 2, pp.169-183,2012.

[37] A. Srinivasan, J. Teitelbaum and J. Wu,"DRBTS: Distributed Reputation-based Beacon Trust System" *in the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06*), Indianapolis, USA, 2006.

[38] Junqi Zhang, Rajan Shankaran, Mehmet A. Orgun, Vijay Varadharajan and Abdul Sattar,"A Dynamic Trust Establishment and Management Framework for Wireless Sensor Networks" *in IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, pp. 484 -492, 2010.

[39] Pengzhi Shi, Haiguang Chen,"RASN: Resist on-off Attack for Wireless Sensor Networks" in 2nd International Conference on Computer Application and System Modeling "published *by Atlantis Press, Paris, France*, pp. 0690 to 0693, 2012.

[40] Sorav Bansal, Mary Baker, "Observation-based Cooperation Enforcement in adhoc networks" pp702-708, 2003.

[41] Guoxing Zhan, Weisong Shi, and Julia Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs" *in IEEE Transactions on Dependable and secure computing* vol.9, pp.184-196,2012.

[42] Younghun chae, "Redeemable reputation based secure routing protocol for wireless sensor networks*", a thesis in university of rhode island*, pp.1-55,2012.

[43] Félix Gómez Mármol, Gregorio Martínez Pérez,"Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems" *in Computer Standards & Interfaces* Vol.no32, pp.185–196,2010.

[44] A. Boukerch, L. Xu , K. EL-Khatib, "Trust-based security for wireless ad hoc and sensor network" *in Computer Communications Vol no* 30 , pp. 2413–2427,2010.

[45] Javier Lopez , Rodrigo Roman, Isaac Agudo, Carmen Fernandez-Gago, "Trust management systems for wireless sensor networks:" *in Best practices in Computer Communications* Vol no 33 ,pp. 1086–1093,2010.

[46] Sudip Misra, Ankur Vaish "Reputation-based role assignment for role-based access control in wireless sensor networks*" in Computer Communications* Vol.no. 34, pp. 281–294, 2011.

[47] Kevin hoffman, David zage, Cristina nita-rotaru," A Survey of Attack and Defense Techniques for Reputation Systems " in ACM Computing Surveys, Vol. 42, No. 1, Article 1, December 2009.