Survey of Various Trust Models and Their Behavior in Wireless Sensor Networks

V. Umarani1, K. Soma Sundaram2
1,2Jaya Engineering College, Tamilnadu, India

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 identify malicious, selfish and compromised nodes. It supports the decision making processes in wireless sensor networks such as pre key-distribution, data aggregation, sink node selection and self reconfiguration of sensor nodes. This paper discussed the general structure, design issues, trust metrics and the corresponding attacks and defense mechanisms of trust model. It also discusses various trust models used in decision making process of Wireless Sensor Networks.

Keywords — Attacks, Security, Trust metrics, Trust model, Wireless sensor network

I. INTRODUCTION

Wireless sensor network (WSN) 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 where reputation is opinion about others. Trust is a belief 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 2 deals with classification of trust, some of the most widely used trust metrics and attacks identified, section 3 discusses the structure of trust model, section 4 describes the major issues in constructing trust model and section 5 reviews various trust models discussed in the literatures.

II. TRUST CLASSIFICATION, METRICS AND ATTACK IDENTIFICATION

In wireless sensor network, trust specifies the reliability or trust worthiness of sensor node. Trust 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 WSNs is known as data trust. Some of the classification is shown in Figure I.
There are several trust metrics taken by trust model to calculate the trust value. Table I discusses some of the trust metric monitored by trust model and the attack addressed by corresponding trust metric.

### Table I

<table>
<thead>
<tr>
<th>Trust metrics</th>
<th>Monitored behavior</th>
<th>Attack addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Packets forwarded</td>
<td>Data message / packet forwarding</td>
<td>Black hole, Sink hole, Selective forwarding</td>
</tr>
<tr>
<td>Control packets forwarded</td>
<td>Control message forwarding</td>
<td>Control/Routing message dropping</td>
</tr>
<tr>
<td>Data packet / Message precision</td>
<td>Data integrity</td>
<td>Data message modification</td>
</tr>
<tr>
<td>Control packet / Message precision</td>
<td>Control packet integrity</td>
<td>Sybil attack and any attack based on routing protocol message modification</td>
</tr>
<tr>
<td>Availability based on beacon/hello messages</td>
<td>Timely transmission of periodic routing information reporting link/node availability</td>
<td>Passive eavesdropping, selfish node, Hello flood attack</td>
</tr>
<tr>
<td>Network layer Acknowledgements</td>
<td>To check successful transmission of message</td>
<td>End to End forwarding, Colluding adversaries</td>
</tr>
<tr>
<td>Packet address modified</td>
<td>Address of forwarded packets</td>
<td>Sybil, Wormhole</td>
</tr>
<tr>
<td>Cryptography</td>
<td>Capability to perform encryption</td>
<td>Authentication attacks, Sniffing attack</td>
</tr>
<tr>
<td>Routing protocol execution</td>
<td>Routing protocol specific actions (reaction)</td>
<td>Misbehaviors related to specific routing protocol actions</td>
</tr>
<tr>
<td>Battery life time</td>
<td>Remaining power sources</td>
<td>Node availability and Position, traffic analysis attack</td>
</tr>
</tbody>
</table>

### III. STRUCTURE OF TRUST MODEL

In wireless sensor networks, trust model 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 Figure II.

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.

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.
The main advantages and disadvantages of trust model are listed in Table II.

**Table II**

<table>
<thead>
<tr>
<th>Structure</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized</td>
<td>Least computational overhead and least</td>
<td>Most Communication overhead, least reliable, lack of</td>
</tr>
<tr>
<td></td>
<td>memory usage</td>
<td>scalability</td>
</tr>
<tr>
<td>Distributed</td>
<td>Most reliable and scalable</td>
<td>Most computational overhead</td>
</tr>
<tr>
<td>Hybrid</td>
<td>Less communication overhead than</td>
<td>Large computational overhead than centralized, large</td>
</tr>
<tr>
<td></td>
<td>centralized and less memory</td>
<td>memory requirement than centralized, less reliable and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>scalable compared to distributed</td>
</tr>
</tbody>
</table>

**IV. DESIGN ISSUES IN TRUST MODEL**

Trust model can be designed by considering the three major components such as information gathering, information modeling and decision making. Each stage has several issues that can be considered carefully in design of trust model in wireless sensor networks [2]. Some of them are listed below,

**A. Information Gathering**

Information gathering is a process in which a node collects information about other nodes that is interested. The main task is to determine type of information should be collected about other neighboring nodes, reputation metrics used to find the behavior of node and how are they distributed. 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 modelling**

It specifies how node calculates reputation value of other nodes which are participating in the networks. Trust system may be a centralized, distributed or Hybrid. In centralized approach is not carefully designed, because single point of failure and is not scale well. In distributed approach, each node calculates reputation values itself and scale well. Hybrid approach is combination of centralized and distributed approach.
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.

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. VARIOUS TRUST MODELS IN WIRELESS SENSOR NETWORKS

Trust plays an important role in human life environments and virtual organizations. Trust is an important issue in distributed system. 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 WSN, 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. Some of them are as follows.

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 Retrust [39] is reputation agent based framework for WSN to incorporate on/off attack resisting model which is improved model of RFSN.

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 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.

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 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 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 trust-based secure data aggregation protocol (TBS)[27] used to select the aggregators 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 in WSN [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 addition encouragement and multiplication punishment (AEMP) [19] is a new routing trust based protocol to enhance WSN 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 RTD 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 networks.

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 [6,7,8,9,11] focused on monitoring, detect malicious behaviors, [12,13,15,18] improve collaboration among sensor nodes, provide reliable communication, [18,19,21],[23,24,25] and [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 [6,7,8,11,12,13] and [15,18,19,30,33,34,35] 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. 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.

<table>
<thead>
<tr>
<th>Trust Model</th>
<th>Purpose</th>
<th>Structure</th>
<th>Trust computation</th>
<th>Data Gathering</th>
<th>Observation</th>
<th>Data Distribution</th>
<th>Punishment</th>
<th>Simulator / tool used</th>
<th>Misbehavior prediction</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFSN[6]</td>
<td>To monitor misbehaviors in network</td>
<td>Distributed and cooperative</td>
<td>Beta distribution approach</td>
<td>Reputation</td>
<td>Self to neighbor and neighbor to neighbor</td>
<td>yes</td>
<td>yes</td>
<td>TRM Sim-WSN</td>
<td>Selfish/malicious routing, packet forwarding</td>
</tr>
<tr>
<td>ATRM [9]</td>
<td>To minimize overhead.</td>
<td>Hierarchical, Certificate based</td>
<td>Agent based</td>
<td>Reputation</td>
<td>Mobile Node(MN) to Sensor node(SN),SN to MN</td>
<td>Optimal threshold</td>
<td>no</td>
<td>NS2</td>
<td>Misbehavior attack</td>
</tr>
<tr>
<td>DRBTS [37]</td>
<td>To monitor misbehaviors in network</td>
<td>Distributed and cooperative</td>
<td>quorum voting approach</td>
<td>Reputation</td>
<td>Self to neighbor and neighbor to neighbor</td>
<td>BN to SN, BN to BN</td>
<td>yes</td>
<td>JSIM</td>
<td>Selfish/malicious routing and packet forwarding</td>
</tr>
<tr>
<td>AEMP [19]</td>
<td>To provide secure routing</td>
<td>Distributed</td>
<td>Weighted approach</td>
<td>Reputation</td>
<td>Base Station(BN) to SN</td>
<td>BN to SN</td>
<td>yes</td>
<td>Mat lab</td>
<td>Selfish/malicious routing</td>
</tr>
<tr>
<td>RDAT [14]</td>
<td>To improves the reliability of data aggregation</td>
<td>Distributed</td>
<td>Beta distribution</td>
<td>Functional Reputation</td>
<td>Self to neighbor and BN to SN</td>
<td>false positive to neighbor</td>
<td>no</td>
<td>TOSSIM</td>
<td>False injection/compromised attack</td>
</tr>
<tr>
<td>TRM-IoT [15]</td>
<td>To establish collaboration among nodes.</td>
<td>Distributed and Behavior based</td>
<td>Fuzzy</td>
<td>Reputation</td>
<td>Self to neighbor</td>
<td>SN to SN</td>
<td>no</td>
<td>NS3</td>
<td>Selfish/malicious routing</td>
</tr>
<tr>
<td>BTRM [12]</td>
<td>To select most trust worthy nodes.</td>
<td>Distributed</td>
<td>Ant Colony</td>
<td>Reputation</td>
<td>Self to neighbor ,neighbor to neighbor</td>
<td>SN to ant ,ant to SN</td>
<td>yes</td>
<td>TRM Sim-WSN</td>
<td>Malicious misbehavior</td>
</tr>
<tr>
<td>DTLSRP [26]</td>
<td>To find trust based routing</td>
<td>Distributed</td>
<td>Weighted</td>
<td>Direct trust</td>
<td>SN to neighbor ,Neighbor to SN</td>
<td>yes</td>
<td>No</td>
<td>Mat lab</td>
<td>Routing attacks</td>
</tr>
<tr>
<td>TMA [31]</td>
<td>To minimize communication and storage overhead.</td>
<td>Behavior and Certificate based</td>
<td>Weight based</td>
<td>Reputation</td>
<td>SN to Cluster Head(CH) ,CH to CH,CH to SN</td>
<td>Integer number from 1-100</td>
<td>no</td>
<td>NS2</td>
<td>Malicious packet forwarding</td>
</tr>
<tr>
<td>RSDA [32]</td>
<td>To improve accuracy of aggregated data</td>
<td>Distributed</td>
<td>Beta probability Density</td>
<td>Reputation</td>
<td>SN to SN ,SN to BN</td>
<td>positive or negative to SN</td>
<td>no</td>
<td>NS2</td>
<td>Malicious/packet forwarding, misbehavior, replay attack</td>
</tr>
<tr>
<td>LDTS [35]</td>
<td>To improve collaborative processing by detecting malicious behavior</td>
<td>Hierarchical</td>
<td>Weight based Approach</td>
<td>Reputation based</td>
<td>CH-to-CH , BS-to-CH, Cluster member(CM) to CM,CH to CM</td>
<td>Optimal trust threshold</td>
<td>no</td>
<td>Net-Logo based trust engine</td>
<td>Malicious misbehavior</td>
</tr>
<tr>
<td>HTMW [36]</td>
<td>To perform routing and intrusion detection</td>
<td>Hierarchical</td>
<td>Stochastic Petri net</td>
<td>Reputation based</td>
<td>SN to SN, CN to SN, Peer to Peer ,CH to CH</td>
<td>Optimal trust threshold</td>
<td>no</td>
<td>NS2</td>
<td>Malicious behaviors and routing attacks</td>
</tr>
</tbody>
</table>
In each research work, authors use different mechanism for reputation calculation such as beta distribution [6,7,8] and 14,32,46, weighted approach [17,26,27,31,35,38,42], Bayesian approach[21,22,33], ant colony approach[12,13], fuzzy[15,30], agent based[9,39] and so on.

Work [6,7,8,14,32,46] 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], trustworthy 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 malignant and non malignant misbehavior in networking, sensing and data processing. This can improve the security issues to meet specific application demands.

REFERENCES
