A Survey on Trust Models for Secure Data Transmission in Wireless Sensor Networks (WSN)
A. Divya Preetha1 P. Prittopaul2
1P.G. Scholar 2Professor
1,2Department of Computer Science & Engineering
1,2Velammal Engineering College Chennai, India

Abstract—Security is the most questing issue in Wireless Sensor Networks (WSN) now-a-days because of the various attacks on mobile nodes. Although a number of proposals have been reported concerning security in Wireless Sensor Networks, provisioning security remains a critical and challenging task. Trust is an important aspect of Wireless Sensor Networks that enables sensor nodes to cope with uncertainty and uncontrollability caused by the free will of other nodes. However due to the computational complexity constraints and excessive energy consumption, trust computation and management is a highly challenging task. Analyzing the trust level of a node has a positive influence on the confidence with which two sensor nodes communicate since an untrustworthy node can adversely affect the quality and reliability of data. A detailed survey on various trust based routing protocols and various trust computation models is presented in this paper. To boot our work, we have analyzed various works on trust dynamics like trust propagation, prediction and aggregation models, and the impact of trust on various security services and the influence of network dynamics on trust dynamics.

Key words: Wireless Sensor Network, Trust Threshold, Trust Computation, Propagation, Aggregation, Trust Dynamics

I. INTRODUCTION

Sensor Networks are the key to the creation of smart spaces, which embed information technology in everyday home and work environment. Wireless Sensor Network (WSN) is a network that consist of multiple battery operated sensor devices with sensing, computation, and wireless communications capabilities. The main aim of Wireless Sensor Network (WSN) is to collect data from the environment [1]. WSN includes many different types of sensors such as seismic, low sampling rate magnetic, thermal, visual, infrared, acoustic and radar, which are able to monitor a wide variety of ambient conditions [2]. WSN finds its applications in military, environment, health, home and other commercial areas.

Wireless Sensor Network (WSN) is employed in harsh environments where pure human access and monitoring cannot be easily scheduled or efficiently managed [3]. Wireless sensor networks are employed mostly in public and uncontrolled areas; hence security is a major challenge [4]. The traditional security mechanisms like cryptography, authentication, confidentiality and message integrity can resist external attacks like eavesdropping, message replay and fabrication of messages. But it cannot resolve internal attacks which are caused by the captured nodes. To facilitate secure communication, we need to ensure that all communicating nodes are trusted.

Trust is defined as the belief level that one sensor node puts on another node for a specific action based on the previous observation of behaviour [5]. A trust model supports decision making in a Wireless Sensor Network (WSN) such as pre key-distribution, data aggregation, sink node selection and self-reconfiguration of these sensor nodes. Trust model encourages trustworthy nodes to communicate bit it discourages untrustworthy nodes to even participate in the network [6]. Trust also increases network lifetime, throughput and resilience in a WSN. Trust may be subjective or objective depending on the task. In general, trust is classified as behavioural or computational trust based on where it is used. Behavioural 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 three primary aspects associated with evaluating trust in distributed networks are as follows. First, trust offers an incentive for good behaviour. Creating an expectation that sensor nodes will “remember” one’s behaviour will cause sensor nodes to act responsibly. Second, trust evaluation provides a prediction of one’s future behaviour. This prediction protects trusted nodes from communicating with less trustworthy nodes. Third, the trust evaluation results can be directly applied to detect selfish and malicious nodes in the network.

The rest of the paper is organized as follows. Section II provides a summary of the various trust based routing protocols. Section III describes the fundamental elements in trust evaluation system that includes trust definition, trust metrics and trust models. In Section IV, the various attacks and protection techniques for trust evaluation system is presented. The conclusion is drawn in Section V

II. TRUSTED ROUTING IN WIRELESS SENSOR NETWORKS (WSN)

Various routing, power management, and data dissemination protocols have been specifically designed for WSNs where energy consumption is an essential design issue.

A. Classification of Routing Protocols

![Routing Protocols Diagram]

- Path Establishment
- Network Structure
- Protocol Operation
- Initiator of Communication

1. Source-based
2. Destination-based
3. Query-based
4. Negotiation-based
5. Based on Coherence

- Multipath based
- Flat
- Hierarchical
- Location-based

- Proactive
- Reactive
- Hybrid
Fig. 1: Classification of Routing Protocols in WSN
The three main categories of routing protocols are data-centric, hierarchical and location-based. Fig. 1 shows the classification of the routing protocols.

B. Structure of Trust Model
In a network, trust helps a node to determine whether its neighbour node is uncooperative or malicious [27]. In an Ad-hoc network, trust plays a major role in detecting misbehaviours, routing and resource sharing. The advantages and disadvantages of a trust model are given in Table I.

Table 1: The Structure of a Trust Model- Pros and Cons

<table>
<thead>
<tr>
<th>Structure</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized</td>
<td>Less computation overhead and memory usage</td>
<td>Communication overhead, less reliable and no scalability</td>
</tr>
<tr>
<td>Distributed</td>
<td>Reliable and scalable</td>
<td>Computation overhead</td>
</tr>
<tr>
<td>Hybrid</td>
<td>Less communication overhead than centralized</td>
<td>Large computation overhead and memory requirements than centralized; less reliable and scalable than distributed</td>
</tr>
</tbody>
</table>

C. Various Trust Models
In WSN, trust plays a major role in detecting a malicious node [36]. Table II shows various techniques that can be used to build a trust model in sensor networks:

Table 2: Trust Models in WSN

<table>
<thead>
<tr>
<th>Model</th>
<th>Purpose</th>
<th>Structure</th>
<th>Computation</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSDA</td>
<td>To amend accuracy of aggregated data</td>
<td>Distributed</td>
<td>Beta probability</td>
</tr>
<tr>
<td>LDTTS</td>
<td>To help collaborative processing by detecting malicious behaviour</td>
<td>Hierarchical</td>
<td>Density</td>
</tr>
<tr>
<td>HTMWM</td>
<td>To execute routing and intrusion detection</td>
<td>Hierarchical</td>
<td>Stochastic Petri net</td>
</tr>
</tbody>
</table>

III. TRUST EVALUATION BASICS
In order to compute the trust level on nodes, we need to understand trust definition, metrics and various trust properties that are employed in trust computations [37].

A. Definition of Trust
In literature, several definitions are given to trust. Trust is always defined by reliability, utility, availability, risk, quality of services and other concepts.

1) Trust as a Belief:
Trust is defined as the belief level that one sensor node puts on another node for a specific action based on the previous observation of behaviour [5].

2) Trust as a Probability:
Trust is a particular level of the subjective probability with which one party assesses that other party will perform a particular action [19].

3) Trust as a Transitive Relationship:
Trust is a weighted binary relationship between two sensor nodes.

4) Trust as a Risk Factor:
[20] states that trusting behaviour occurs when an individual node perceives an ambiguous path, the result of which could be good or bad, and the occurrence of the good or bad result is contingent on the actions of another node. [21], [22] defines trust as a bet about the future contingent action of other nodes.

B. Trust Metrics
The various metrics that are used in trust evaluation are categorized as follows

1) Trust Scale:
The level of trust can be measured using continuous or discrete data. Trust can be measured by a continuous value in [0,1] or as a discrete value in [-1,1]. Trust can also be measured using threshold based approaches. A node is considered to be trustworthy if the trust value of that node exceeds a particular threshold.

2) Trust Facets:
In [23], a confidence value in the interval [0,1] and a trust value in the interval [0,1] denote the trustworthiness of a node. Trust can also be measured as a triplet \((b,d,u) \in [0,1]^3\) where \(b, d\) and \(u\) denote belief, disbelief and uncertainty respectively.

3) Trust Logics:
Probability can also be used as a trust metric. The ratio between the numbers of packets forwarded correctly to the
total number of packets received can also be used as a trust metric. The bad and good experiences are used in Beta distribution to obtain the trust value.

Trust is always established between two parties for a specific action. The first party can be called as subject and the second party can be called as object. A trust relationship is represented by \( \text{subject: agent, action} \).

C. Trust Properties

The three main properties of trust [5] are as follows:

1) Asymmetry:
   Asymmetry implies that if node A trusts node B, it does not necessarily mean that node B trusts node A.

2) Transitivity:
   Transitivity implies that trust value can be passed along a path of trusted nodes. If node A trusts node B and node B trusts node C, it can be inferred that node A trusts node C at a certain level.

3) Composability:
   Composability implies that trust values received from multiple available paths can be composed together to obtain an integrated value.

D. Trust Blocks

![Fig. 2: Relationship among various trust blocks](image)

First, the trust value of all the nodes will be computed based on certain metrics and recommendations. The trust computation can be centralized or distributed.

Then the computed trust values will be propagated in the network in order to establish trust between nodes that are not in immediate contact.

<table>
<thead>
<tr>
<th>Title &amp; Year</th>
<th>Perspective Employed</th>
<th>Trust &amp; Performance Metric</th>
<th>Advantages</th>
<th>Complexity</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct Trust</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enhancing Trust Aware Routing by False Alarm Detection and Recovery (2014)[31]</td>
<td>Finite State Machine (FSM) Model</td>
<td>Trust is categorized as ( [T,S,U] ), S is sub-categorized as SU and ST</td>
<td>Improved network lifetime, routing &amp; false alarm recovery performance</td>
<td>Additional overhead in maintaining Trust Threshold for Suspicious nodes and Untrustworthy nodes</td>
<td>Fails when a critical node fails and no alternate path can be found</td>
</tr>
<tr>
<td>A Novel Approach to Trust Management in Unattended Wireless Sensor Networks (July 2014)[30]</td>
<td>Subjective Logic Framework</td>
<td>Trust is measured as a triplet ( T{B,D,U} )</td>
<td>Resilient to major attacks like ADV-Del, Noise, Homo, Hybrid</td>
<td>Difficulty in setting up a suitable threshold value</td>
<td>When threshold is small, more correct trust opinions are considered as outliers and vice versa</td>
</tr>
</tbody>
</table>

**HYBRID TRUST**

| Direct Trust |
|--------------|------------------|-----------------------|-------------|------------|-------------|
| HYBRID TRUST |
| Building a Trust Aware Dynamic Routing Solution for Wireless Sensor | Trust Aware Dynamic Routing Framework | Trust is measured in \([0,1]\). Trustworthiness is derived from Reputation (RE) and Risk(RI) | Significantly improves network throughput, reliability even under attacks like message tampering/modification & selective forwarding | Energy consumption is high since trust value is calculated based on historical data, recent short | When black hole nodes positioned in a straight line collide, nodes in the middle may not be detected due to lack of |
Networks (2011) | ReTrust : Attack-Resistant and Lightweight Trust Management for Medical Sensor Networks (July 2012) | Collection Tree Protocol | Trust is considered to be an integer in [0, lam]. Here lam=100. Trust value is denoted by T(subject,agent,action) | .Identify malicious behaviour & exclude it. .Improve network performance. .Defend on-off attack & bad mouthing attack | The usage of checking method to isolate bad recommendation | Network throughput decreases as the number of malicious nodes increases

Trust Management for Defending On-Off Attacks (April 2015) | Trust Redemption Scheme & Dynamic Sliding Window Scheme | Trust is measured in [0,1]. Predictability trust & Redemption factor | .Badly reputed nodes have an opportunity to regain trust. .Average throughput is high. Since almost all nodes are trusted, the hop count increases thereby consuming more energy for communication. | As the size of the Bad Behaviour Window (BBW) increases, the trust value decreases automatically

### Table 3: Comparison of Different Distributed Trust Computing Mechanisms

During trust propagation, the trust value from multiple paths can be aggregated to get a combined trust value that can be stored in history. This can be used in trust prediction which in turn can be used in the applications that need security.

**IV. TRUST COMPUTATIONS**

The three components of trust computation include ‘experience’, ‘recommendation’ and ‘knowledge’ [24]. Experience is directly measured by immediate neighbours and kept updated at regular intervals in the trust table. The existing trust table is propagated among the network as ‘recommendation’. Knowledge component includes the previously evaluated trust at a regular interval [37]. Trust computation can be either centralized or distributed.

#### A. Distributed Trust Computation

Distributed trust computation is classified as direct, indirect and hybrid trust.

1) **Direct Trust:**

Every node observes their neighbours for their event reports and stores the reports in their knowledge cache. A trustor node (trust measuring node) compares its own observation report on event with the observation report it received from the trustee node. Trust factor is determined based on the amount of deviation between the observation reports.

Trust of a particular node $x$ is calculated [32] by a node $y$ as follows:

$$ T = W(R_p) \times R_p + W(R_s) \times R_s + W(R_f) \times R_f + W(D) \times D $$

(1)

where $W(.)$ is the weight assigned to a particular event, $R_p$, $R_s$, $R_f$, $D$ are normalized route reply misbehaviour factor, route request misbehaviour factor, route error misbehaviour factor and data delivery misbehaviour factor respectively.

$$ R_p = R_{ps} - R_{qs} + R_{pf} $$

$$ R_s = R_{ps} - R_{qs} + R_{sf} $$

$$ R_f = R_{ps} - R_{qs} + R_{qf} $$

$$ D = D_p - D_s - D_f $$

where $R_{ps}$, $R_{qs}$, $R_{sf}$ and $D_p$ are the number of successful: route reply acknowledgement packets, route request acknowledgement packets, route error acknowledgement packets and data delivery acknowledgement packets, respectively. Similarly $R_{pf}$, $R_{qf}$, $R_{qf}$ and $D_f$ are the number of failed packets.

Every node measures the trust of other nodes by observing their behaviour. Over the time, these experiences will become stale. Therefore, $x$ will assign some weight value to the past history.

<table>
<thead>
<tr>
<th>Title &amp; Year</th>
<th>Context In Use</th>
<th>Trust &amp; Performance Metric</th>
<th>Advantages</th>
<th>Complexity</th>
<th>Performance &amp; Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Based Trust Management Scheme for Clustered Wireless Sensor Networks (2009)</td>
<td>Sliding Window Scheme</td>
<td>Trust value is an integer between 0 and 100. Trust is quantized into three states: trusted, untrusted, uncertain</td>
<td>.Less communication overhead by usage of trust state. .Each communication don't require extra communication to calculate the trust value</td>
<td>As the number of clusters increases, the memory consumption requirement at the CH increases</td>
<td>More suitable only for large scale WSN with small size of clusters</td>
</tr>
</tbody>
</table>

Communication Trust Based Watchdog .CH sends the key Updating sensor Will not give good
2) Recommendation Based Trust:
Trust relationships on nodes are established based on recommendations alone. Every node will monitor its one hop neighbour nodes and generate a “trust report” based on the neighbour nodes’ behaviour. Initially all nodes will have a random unknown trust level on other nodes. Once the trust report is generated it will be either broadcasted to all nodes or it can be flooded controllably in the network. Recommendation reliability and recommendation familiarity [5] are used to filter false recommendations and to detect malicious nodes.

3) Hybrid Method:
Trust on a node is computed based on direct experience and also recommendations from other nodes. Node x’s trust [33] on node y is given by

\[ T_{xy} = \alpha T_x + \beta T_0 \]

where \( \alpha \) and \( \beta \) are such that \( \alpha + \beta = 1 \). \( T_x \) is computed by monitoring node y for total packets dropped by y, packet forwarding delay by y, packets misrouted by y and the packets wrongly injected by y. \( T_a \) is the collective trust evaluation by all nodes on y.

Comparison of various distributed trust computing schemes is provided in Table III.

B. Centralized Trust Establishment
Centralized trust establishment scheme assumes a trust agent (TA) that can be accessible by all nodes in the group. Trust Agent can either compute trust for the whole network or can assist nodes in their trust computation by providing initial trust value on target nodes. A centralized cluster head based trust computation [34] works as follows. The cluster head provides every node in the cluster with the initial trust value on every other node. Each node will combine its own calculated trust value based on experience with the initial trust value obtained from the cluster head. Node i evaluates the trust value of node j as follows:

\[ \varphi(i,j) = T(i,j) \times \alpha + T(H_j) \times (1 - \alpha) \times \beta \]

where \( T(i,j) \) is the trust value of node j calculated by node i based on successful data delivery rate and experience rate. \( T(H_j) \) is the node j’s initial trust value obtained from the cluster head. \( \beta \) is the malicious factor (\( \beta = 0 \) denotes malicious and \( \beta = 0 \) denotes non-malicious).

The trust value of the target node will be evaluated by all other nodes and sent to the cluster head. The cluster head will multiply each value with the trust value of the provider and the average of them determines the final trust value. This is given as trust certificate to all nodes in the cluster.

An agent-based trust and reputation scheme is proposed is [25], [26] for MANET. It is assumed that there are n number of reputation assistants. To evaluate the trust value of a neighbour node x, the node C has to query its reputation assistants about this neighbouring node x. Once node C receives the trust value from its reputation assistants, it uses the weighted means to measure the node’s final trust thereby making the corresponding decision. The final trust of C on X(T) is given by

\[ \text{Trust}_{AVG} = \frac{\sum_{i=1}^{n} \text{Trust}_{AI,Xn}}{n} \]

\[ w_i = \frac{\text{Trust}_{AI,Xn}}{\text{Trust}_{AVG}} \]

\[ T = (\text{Trust}_{C,X} + \sum_{i=1}^{n} w_i \times \text{Trust}_{RAI,X})/(n+1) \]

Where \( \text{Trust}_{AVG} \) is the average agent (reputation assistant) trust on node X. \( \text{Trust}_{RAI,X} \) is the trust of reputation assistant i on X. \( w_i \) is the weight given to trust value obtained from assistant i and \( \text{Trust}_{C,X} \) is the self-measured trust of node C on X.

Comparison of various centralized trust computing schemes is provided in Table IV.

C. Attacks in Trust Model
A list of the possible trust based attacks in Wireless Sensor Network is given below:
1) Bad Mouthing Attack:
Bad Mouthing attack involves a node giving bad recommendation about other nodes intentionally.

2) Denial of Service Attack (DoS):
The attackers send as much trust recommendations as possible to consume the resources of the trust calculating nodes.

3) On-off Attack:
The malicious nodes behave good and bad intentionally based on the importance of the situation.

4) Sybil Attack:
A malicious node creates several fake IDs. The fake IDs take the blame that should be given to the actual malicious node.

5) Conflicting Behaviour Attack:
The malicious node behaves differently towards different nodes. That is, it can give good recommendation about a node to one group of nodes and bad recommendation about the same node to the other set of nodes.
6) Camouflage Attack:
The dishonest users attempt to build up trust by always reporting as per the observed majority. After earning enough trust value, they behave dishonestly for specific occasions.
7) New Comer Attack:
The attacker just leaves the system and joins again hoping to flush out the previous bad history and to accumulate new and good trust value.
8) Collusion Attack:
This attack is launched by more than one malicious node collaborating and providing false recommendations about other nodes.

D. Trust Dynamics:
Trust is a dynamic phenomenon. It changes with time, experience and the state of various sources it is based on. Evolution of trust over time is called trust dynamics and is characterized by the following components: trust propagation, prediction and aggregation.
1) Trust Propagation:
Energy consumption of nodes can be reduced if the computed trust value gets propagated in the network. Recommendation is the simplest form of trust propagation. Recommendation is usually from a single-hop neighbour while trust propagation can be multi-hop. Trust propagation is based on the transitivity property of trust.

<table>
<thead>
<tr>
<th>Trust Aggregation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title &amp; Year</td>
</tr>
<tr>
<td>Secure Trust Reputation with Multi-Criteria Decision Making for WSN Data Aggregation (2011) [29]</td>
</tr>
<tr>
<td>Trust Aware In-Network Aggregation for Wireless Sensor Networks (2009)</td>
</tr>
<tr>
<td>Trust-Based Secure Aggregation in Wireless Sensor Networks [28]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trust Propagation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title &amp; Year</td>
</tr>
<tr>
<td>An Improved Intrusion Detection Scheme Based on Weighted Trust Evaluation for WSN (2010)</td>
</tr>
<tr>
<td>Trust Based Intrusion Detection in Wireless Sensor Networks (2011)</td>
</tr>
<tr>
<td>LDTS : A Lightweight and Dependable Trust</td>
</tr>
</tbody>
</table>
System for Clustered Wireless Sensor Network (June 2013) [17] | propagate trust from CM to CH & CH to BS | interval between 0 and 10 | overhead | to store the feedback matrix | with a large size of clusters
---|---|---|---|---|---
Trust Prediction

- **Markov Chain Based Trust Management Scheme for Wireless Sensor Networks (Dec 2014)**
  - Adaptive memory factor is used to predict trust values
  - Trust is measured as a five-tuple Markov model $\Omega=(R,V,Q,^\pi,\pi)$. Markov chain reduces the impact of environment on evaluating node’s state
  - \[ y = \text{Agrre}(x_1, x_2, \ldots, x_n) \]

  The important conditions [35] for aggregation operator $\oplus$ are as follows:
  - **Boundary Condition:** $\text{Agrre}(0, 0, \ldots, 0) = 0, \text{Agrre}(1, 1, \ldots, 1) = 1$
  - **Non Decreasing Condition:** $\forall x_i > x_j \forall i \\text{Aggre}(x_1, x_2, \ldots, y_i, \ldots, x_n) > \text{Agrre}(x_1, x_2, \ldots, x_n)$

- **Trust Prediction:**
  - Trust Prediction is a method of predicting unknown trust value between two nodes using the present and past behaviour of nodes and also the recommendation received from other nodes.

### Table 5: Various Trust Aggregation, Propagation and Prediction Techniques

| **2) Trust Aggregation:** | When trust values are propagated through multiple paths, multiple values of this value are received at the destination. Aggregation can be done at the destination to combine these values into a single trust value. This trust aggregation is based on the composability property of trust. Aggregation plays a major role in suppressing some malicious activities. Trust Aggregation problem consists of aggregating n-tuples of observed trust values, all belonging to a given set $(x_1, x_2, \ldots, x_n)$, into a single value of the same set (y) as follows:
| **3) Trust Prediction:** | Trust Prediction is a method of predicting unknown trust value between two nodes using the present and past behaviour of nodes and also the recommendation received from other nodes. |

V. CONCLUSIONS AND FUTURE WORK

Trust is an important area of research. The goal of this paper is to provide multiple perspectives on the concept of trust, an understanding of the properties to be considered in developing a trust metric, and how trust should be computed. We then presented a survey of various trust computing metrics. We then analyzed trust dynamics such as trust propagation, aggregation and prediction. We hope that in the near future we will bring a set of fundamental principles for building trust and its issues. These will be realized in practical and commercial applications too. We have also proposed a trust model that uses only direct trust based on three factors like Channel State Information, Link Residual Life and energy of the receiver node to calculate the trust value of a sensor node. This proposed Self-Evaluating Trust Model in WirelessHART Standard saves energy, improves network lifetime and improves performance of the network. Trust computation and performance metric of this proposed work can be found better in our next paper.

REFERENCES


