A Trust Management Architecture for Hierarchical Wireless Sensor Networks

Junqi Zhang\textsuperscript{1,2}, Rajan Shankaran\textsuperscript{1}, Mehmet A. Orgun\textsuperscript{1}, Vijay Varadharajan\textsuperscript{1} and Abdul Sattar\textsuperscript{2}

\textsuperscript{1}Department of Computing, Macquarie University, Sydney, Australia
\{janson, mehmet, rshankar, vijay\}@science.mq.edu.au
\textsuperscript{2}School of Information and Communication Technology, Griffith University, Brisbane, Australia
A.Sattar@griffith.edu.au

Abstract—Security and trust are fundamental challenges when it comes to the deployment of large wireless sensor networks. In this paper, we propose a novel hierarchical trust management scheme that minimizes communication and storage overheads. Our scheme takes into account direct and indirect (group) trust in trust evaluation as well as the energy associated with sensor nodes in service selection. It also considers the dynamic aspect of trust by introducing a trust varying function which could give greater weight to the most recently obtained trust values in the trust calculation. The proposed framework can be extended to such dynamic mobile inter-cluster wireless sensor network environments.

I. Introduction

Wireless Sensor Networks (WSNs) comprise of a large number of spatially distributed tiny autonomous devices that cooperatively monitor and react to environmental conditions and send the collected data to a command center using wireless channels. Due to limited resources of WSNs, it is challenging to incorporate basic security functions such as authentication, privacy, and key distribution. As a result, wireless sensor networks are prone to different types of malicious attacks, such as denial of service, routing protocol attacks as well as replay attacks. Traditional crypto schemes are incapable of preventing such types of malicious attacks. We need to enhance security protocols with trust and security management techniques. However traditional trust management schemes developed for wired and wireless networks may not be suitable for networks with small sensor nodes due to limited bandwidth and stringent node constraints in terms of power and memory.

There are several proposals for trust management for WSNs [1], [2], [3], [4], [5], [6], [7]. None of these proposals consider the all the requirements/constraints of trust management for WSNs Some approaches such as the one proposed in [8] do not take dynamic aspects of trust into consideration. The focus of this paper will be to develop a formal model for modeling trust in hierarchical ad hoc sensor networks [9] to enable mobile sensor nodes to form, maintain and exchange trust opinions with minimal overheads in terms of complex computations at sensor nodes.

This paper is organized as follows. Section 2 presents our new trust scheme for hierarchical ad-hoc wireless sensor networks. Section 3 provides a comparison of our proposed trust scheme with the existing trust management schemes. Finally, Section 4 concludes the paper with a brief summary.

II. Trust Management for WSNs

In this paper, we use the super node based trust management approach [10], [9]. In such schemes, some nodes referred to as super nodes are assumed have more computation power, storage, and power for communication. One example of such a scheme is called a group based trust management scheme (GTMS) proposed in [8] for clustered WSNs. Our scheme is based on this architecture. Our dynamic trust framework builds on the hierarchical architecture of WSNs described in [8] to minimize the nodes’ memory by storing trust information in the cluster head. We employ a decaying trust function which can be used to give more weight to the most recent trust value in the overall trust value computation. We combine behavior based trust and certificate based trust using the pre-deployment knowledge in the establishment of trust relationships. We also allow the nodes to move from one cluster to another by preserving their trust record, thereby making the scheme suitable for dynamic environments wherein the nodes move frequently.

A. Trust Management Architecture

Hierarchical wireless sensor network model was proposed in [11], [12]. This model has been subsequently used by other researchers such as [13], [10], [9], [14]. In this model, a wireless sensor network consists of a command node, cluster heads and numerous sensor nodes which are grouped into clusters [15], [16]. It is assumed that all sensors and cluster head nodes are stationary and the physical location and communication range of all nodes in the network are known. The clusters of sensors can be formed based on various criteria such as capabilities, location and communication range, and the usage of different cluster algorithms and strategies.

Each cluster includes the cluster head (or the cluster leader) and a set of distinct sensors. Each sensor has two main functions: sensing and relaying. Sensors probe their environment and gather data. Then they transmit the collected information to the cluster head directly in one hop or by relaying via a multi hop path. Sensors transmit or relay data only via short-haul radio communication. A cluster head is in charge of its
cluster. It is assumed that each cluster head can reach and control all the sensors in the cluster. Each cluster head receives the information from different sensors, processes the data to extract relevant information, and then sends it to the base station (command node) via long-haul transmission.

Our architecture introduces the notion of a sponsor node as shown in Figure 1. A sponsor node is the initiator of each cooperation, denoted as s. Any node can be a sponsor node based on the application. This sponsor node will find one or more other nodes to cooperate together. A target node is the node chosen by the sponsor node to cooperate for a service, denoted as t. There can be one or more target nodes for each service. The sponsor selects the target using the direct trust value that it has for the target or else it will obtain this information from the cluster head. In our architecture we assume that the cluster head has higher computation power and memory when compared to other sensor nodes. The base station (or command node) is assumed to be totally trusted and virtually has no computational or memory constraints.

![Fig. 1. Trust in WSN Architecture](image)

As shown in Figure 1, each node stores all the direct trust values of other nodes in the same cluster. Each node then sends all the direct trust values of other nodes to the cluster head. Using the direct trust values, the cluster head calculates and stores the indirect (group) trust information for each node in the cluster. In addition, the cluster head also stores its own direct trust value for each node as well as the power (energy) level of each node residing in its cluster. The cluster head then calculates the integrated trust value for each node in the cluster based on the group and cluster head’s direct trust values.

We denote a node using the following tuple \((ID, A, V, T)\), where \(ID\) denotes the identity of the node, \(A\) denotes the attribute set of node \(ID\), \(V\) denotes the value set associated with the attributes, and \(T\) denotes the trust value set of the attributes. To be deemed as trustworthy, a node must make a reasonable effort to perform its network related services in a dependable manner. The network services of a node can be broadly classified into the following three categories: (1) routing/forwarding related, (2) QoS related, and (3) security related. Several attributes for routing and forwarding are highlighted in [17] such as packet drop rate, duplicate packets received, and latency (delay/ delay jitter).

Trust can be represented in several ways. For instance, in [8], trust values have been represented by an integer in the interval between 0 and 100. An unsigned integer uses 1 byte while a real number uses 4 bytes. This means that the representation of trust values \([0, 100]\) can save up to 75 percent of memory space. As a result, the data transmission between nodes is also reduced. Consequently, the power consumption can also be decreased. For the same reason, we also represent trust values as an integer between 0 and 100.

### B. Node Level Trust Management

In our framework, the direct trust value between a sponsor node \(s\) and a target node \(t\) is denoted as \(T_{st}\). Group trust value is denoted by \(G_t\) (calculated from the direct trust values of all the nodes in the cluster) and integrated trust value is denoted by \(I_t\) (calculated based on the direct trust value \(T_{ch,t}\) of the cluster node and the group trust value \(G_t\) where \(ch\) denotes the cluster head). The direct trust value of a target node is calculated based on its multi-attribute trust values. The sponsor node evaluates and records the result of the cooperation with the target node.

The cooperation records are listed as shown in Table I. Each attribute \((A_i, i = 1, 2,..,n)\) has two relevant values: the value of the successes \((S_i, i = 1, 2,..,n)\), and the value of the cumulative cooperations \((CC_i, i = 1, 2,..,n)\). For example, if the cumulative cooperation \(CC_1 = 10\), then \(S_1\) can be any number between 0 to 10.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Number of Successes</th>
<th>Number of Cooperations</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A_1)</td>
<td>(S_1)</td>
<td>(CC_1)</td>
</tr>
<tr>
<td>(A_2)</td>
<td>(S_2)</td>
<td>(CC_2)</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>(A_n)</td>
<td>(S_n)</td>
<td>(CC_n)</td>
</tr>
</tbody>
</table>

Based on the cooperation success records, we can calculate the trust value for attribute \(A_i\) as follows:

\[
t_{A_i} = \left[100 \times \frac{S_i}{CC_i}\right]
\]

where \(0 \leq t_{A_i} \leq 100\) and \([\cdot]\) is the nearest integer function.

We divide time into Time Units. Individual sensor nodes keep track of cooperation records with the other sensor nodes within a certain time frame. The size of the time frame is critical for trust evaluation. The duration of this time frame can be dynamically determined and is influenced by factors such as application requirements and/or resource constraints of each sensor node. Following research in social networks [18] showing that a social relationship beyond family (such as the trust relationship between sensor nodes in our work) will decay...
with time, the older trust value may take less weight in the overall trust value and decay accordingly.

At time $T_k$, the trust value for attribute $i$ is $T_{A_{ik}}$ and during the time unit $t_{k+1}$, the trust value is $t_{A_{ik+1}}$. The trust value at time $T_{k+1}$ can be calculated as follows:

$$T_{A_{ik+1}} = [(100 - \theta)/100] \cdot T_{A_{ik}} + \theta/100 \cdot t_{A_{ik+1}}$$  \hspace{1cm} (2)

where $0 \leq \theta < 100$ and $[.]$ is the nearest integer function. With this formula, the new trust value at time $T_{k+1}$ results from the trust value at time $T_k$ and the trust value during the new time unit $t_{k+1}$. The parameter $\theta$ controls the decay of the older trust value and the contribution of the trust value during the new time unit.

When the trust value in the latest time unit is high, the overall trust value will go down sharply. For instance, suppose that one node turns to bad behavior in one time unit, $T_{A_{ik}} = 90$ and $t_{A_{ik+1}} = 20$, then $\theta = 80$, $T_{A_{ik+1}} = [(100 - \theta)/100] \cdot T_{A_{ik}} + \theta/100 \cdot t_{A_{ik+1}} = 0.2 \cdot 90 + 0.8 \cdot 20 = 34$.

Now we are able to calculate the overall trust value for the target node $t$ with $n$ attributes $A_i, i = 1, 2, ..., n$ for a given sponsor node $s$ as follows:

$$T_{s,t} = \frac{\prod_{i=1}^{n} T_{A_i}}{\prod_{i=1}^{n} T_{A_i} + \prod_{i=1}^{n} (1 - T_{A_i})}$$ \hspace{1cm} (3)

C. Cluster Head Level Trust Management

A cluster head has several roles. Within its cluster, a cluster head stores all the trust records of the nodes in its cluster, and furnishes the integrated trust value to a requesting node. Within the wireless sensor network, a cluster head also records other cluster head trust values. The cluster head is in charge of transferring the trust record of a node when the node moves from one cluster to another. Let us now consider each of these functions in turn.

1) Intra-Cluster Trust Management: Each node transmits the recorded trust values that it has for other target nodes to the cluster head. The cluster head stores all the records for calculating the node’s group trust value. Suppose that there are $n + 1$ nodes in the group including the cluster head. Each of the group member nodes forwards its direct trust values of the other member nodes to the cluster head when one of the trust values is changed. The cluster head maintains these trust values in a matrix form, as shown below:

$$T_{ch} = \begin{bmatrix}
T_{1,2} & T_{2,1} & ... & T_{n,1} \\
T_{1,3} & T_{2,2} & ... & T_{n,2} \\
... & ... & ... & ... \\
T_{1,n} & T_{2,n} & ... & T_{n,n-1}
\end{bmatrix}$$

Each column in the above matrix corresponds to the vector of trust values for the corresponding sensor node. For example, $T_{1,2}$ is the node 2’s direct trust value sent by node 1.

a) Integrated Trust Computation: The integrated trust value computation of a node involves three steps: group trust values, cluster head’s trust value, the base station’s trust value. The group trust values can be derived from the above matrix. The cluster head has its trust value for each node in its cluster group as well. The base station has a trust value for each node that resides in the wireless sensor network (a collection of clusters) as it is the only node in the network that has the complete knowledge necessary to evaluate and assess every function that a sensor node is capable of performing. Each cluster head keeps track of a trust matrix:

$$T_G = \begin{bmatrix}
G_1 & T_{ch,1} & T_{b,1} \\
... & ... & ... \\
G_i & T_{ch,i} & T_{b,i} \\
... & ... & ... \\
G_n & T_{ch,n} & T_{b,n}
\end{bmatrix}$$

where $i = 1, ..., n$ and the $G_i$, $T_{ch,i}$, $T_{b,i}$ are the group trust value of node $i$, the cluster head’s direct trust value for $i$ and the base station’s trust value of $i$.

Given that there are $n + 1$ nodes in the given cluster including the cluster head, the group trust value $G_i$ for node $i$ is calculated as follows:

$$G_i = \frac{\prod_{j=1, \ldots, i-1,j+1, \ldots, n} T_{j,i}}{\prod_{j=1, \ldots, i-1,j+1, \ldots, n} T_{j,i} + \prod_{j=1, \ldots, i-1,j+1, \ldots, n} (1 - T_{j,i})}$$ \hspace{1cm} (4)

Based on the service trust record values of all other nodes, the cluster head can then compute the integrated trust value $I_i$ for each node as follows:

$$I_i = G_i \cdot W_{\text{group}} + T_{ch,i} \cdot W_{ch} + T_{b,i} \cdot W_{\text{base}}$$

Here $W_{\text{group}}$, $W_{ch}$ and $W_{\text{base}}$ are the weights for the corresponding trust values and they can be adjusted dynamically by the cluster head. The weights must add up to 1.

b) Transfer of Integrated Trust to Sponsor Node: We first stipulate that the cluster head also keeps track of the energy levels of the sensor nodes in its cluster in a vector $[E_1, E_2, \ldots, E_n]$ which is used in service selection and load balancing.

When a sponsor node does not have the direct trust value for a target node, it will request the target nodes’ trust values from the cluster head. The cluster head will then send the integrated trust values for all the requested nodes, along with their energy levels. The sponsor node is then able to find the path with higher trust value to perform the required service with the node with the sufficient energy level.

2) Inter-Cluster Trust Management: We assume that the nodes (apart from the cluster heads) in the wireless sensor network are dynamic. They can move from one cluster group to another cluster group. We have been developing a full trust management scheme for such inter-cluster movements, however, due to space limitations, we do not discuss it here.
III. Comparison with Related Work

Table II summarizes the comparison between our proposed trust management architecture (TMA) with the previously proposed GTMS framework [8] in terms of computation, memory requirements and communication overhead. This is because only these two schemes have the similar architecture.

In TMA, by propagating the energy level of a target node along with its trust value, a recipient can decide whether or not to use the services of this target node. On the other hand, in GTMS, there is no such an arrangement. In TMA, we also take advantage of the pre-deployment knowledge. As the sensor networks have infrastructure components such as a base station which can perform centralized management, we can employ certificates to validate new nodes. In addition, our trust management architecture has the ability to consider movement of nodes from one cluster to another.

<p>| TABLE II |</p>
<table>
<thead>
<tr>
<th>Comparison of TMA and GTMS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GTMS</strong></td>
</tr>
<tr>
<td>Communications among Nodes for trust calculation</td>
</tr>
<tr>
<td>Transmission length between Nodes and the Cluster Head</td>
</tr>
<tr>
<td>Communication times for Nodes and the Cluster Head</td>
</tr>
<tr>
<td>Communications for Cluster Heads and the Base Station</td>
</tr>
<tr>
<td>Memory overhead for Nodes</td>
</tr>
<tr>
<td>Memory overhead for Cluster Heads</td>
</tr>
<tr>
<td>Computation overhead for Nodes</td>
</tr>
<tr>
<td>Computation overhead for Cluster Heads</td>
</tr>
<tr>
<td>Trust decay</td>
</tr>
<tr>
<td>Energy level for nodes</td>
</tr>
<tr>
<td>Pre-deployment Certificates</td>
</tr>
<tr>
<td>Enhancing Cluster Head Trust Management</td>
</tr>
<tr>
<td>Dynamic Node Movement</td>
</tr>
<tr>
<td>Multi-hop Routing</td>
</tr>
</tbody>
</table>

IV. Concluding Remarks

In this paper, we have proposed a dynamic trust management architecture for hierarchical wireless sensor networks that reduces the computation and communication requirements of sensor nodes in carrying out trust evaluation. Our scheme incorporates a time window and a decay function that captures the changing nature of trust in trust calculations. Using comparative analysis, we prove that our model has more robust features to support trust in comparison to other similar schemes that aim to achieve the same.

Acknowledgements

This research was supported in part under Australian Research Council’s Discovery Projects funding scheme (project DP0452628), and a Macquarie University Research Development Grant (MQRDG).

References