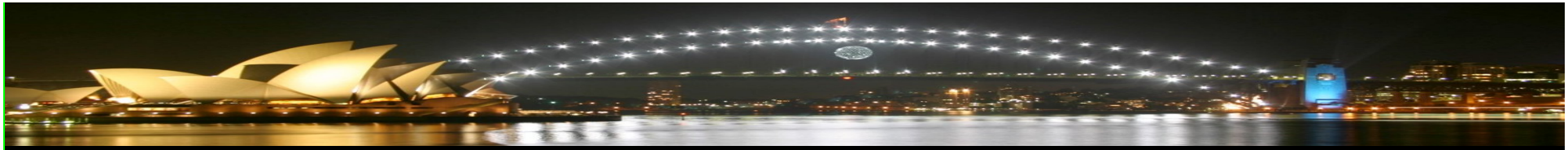


Trust Management Problem in Distributed Wireless Sensor Networks

18 August 2006

12th IEEE RTCSA Conference

Riaz Ahmed Shaikh

Dep. of Computer Eng., KyungHee University

Republic of Korea

riaz@oslab.khu.ac.kr

Kyung Hee University

Agenda

- Introduction
- Motivation
- Problem Statement
- Proposed Solution
- Conclusion
- Future Work

Introduction: Trust

- Definition of Trust:

  "the quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context"

  (T. Grandison and M. Sloma, 2000)

- Traditionally trust is applied in various diverse domains such as e-commerce systems, ad-hoc networks, and peer-to-peer networks.

Introduction: Wireless Sensor Networks

- A wireless sensor network is an emerging technology that is used in various application areas such as health, military, and home etc .
- It typically consists of tiny sized sensor nodes that are densely deployed in an environment. The basic objective of a sensor network is to sense, gather and propagate information about the environmental phenomena.
- Recent widespread uses of sensor networks have evoked the need of proper lightweight trust management schemes.

Introduction: Why we need Trust

- Establishing trust in a network gives two main benefits such as;

Introduction: Motivation

- Traditional research work in wireless sensor networks is mostly based on the assumption of a trusted environment which may not be realistic for every application.

- Traditional trust management schemes that have been developed for wired and wireless ad-hoc networks are not suitable for wireless sensor networks because of higher consumption of resources such as memory and power.

Classification of Trust Management Schemes

✓ Less computational overhead. ✓ Consume Less memory.	✓ Single Point of failure. ✓ Increase communication overhead.
✓ Reliable means no single point of failure. ✓ Scalable.	✓ Increase computational overhead. ✓ Consume large memory.
✓ Less communication overhead than centralized. ✓ Less memory consumption than distributed. ✓ Less computational overhead than distributed. ✓ More reliable and scalable than centralized.	✓ Large computational overhead then centralized. ✓ Large memory requirement than centralized. ✓ Less scalable and reliable than distributed.

Moving Towards Unique Idea

- By looking at the advantages and disadvantages of all three approaches we conclude that neither completely centralized nor completely distributed trust management schemes are appropriate for wireless sensor networks.
- Therefore, hybrid trust management schemes are more suitable for wireless sensor networks.
- Hybrid Approach can be used with the help of clustering topology.

Moving Towards Unique Idea (Cont…)

- Wireless sensor networks use various clustering schemes such as LEACH, HEED, etc, that are used in real world scenarios. The basic objective of these clustering schemes is to reduce the communication cost.
- Moreover, sensor nodes can also be deployed in the form of groups.
- This highlights the fact that these clustering schemes and group deployment, enable sensor nodes to fulfill their responsibilities in a cooperative manner rather than individually.
- Thus one should also consider the trust management as a cooperative business rather than an individual task.

Problem Statement

- Research on trust management scheme for wireless sensor networks is in the infancy state. Hence, in this work, we propose a novel lightweight *group based trust management scheme* (GTMS) for distributed wireless sensor networks that is based on *hybrid trust management* approach.

- We focus on following problem.

Research Challenges

- Research challenges for this problem are:

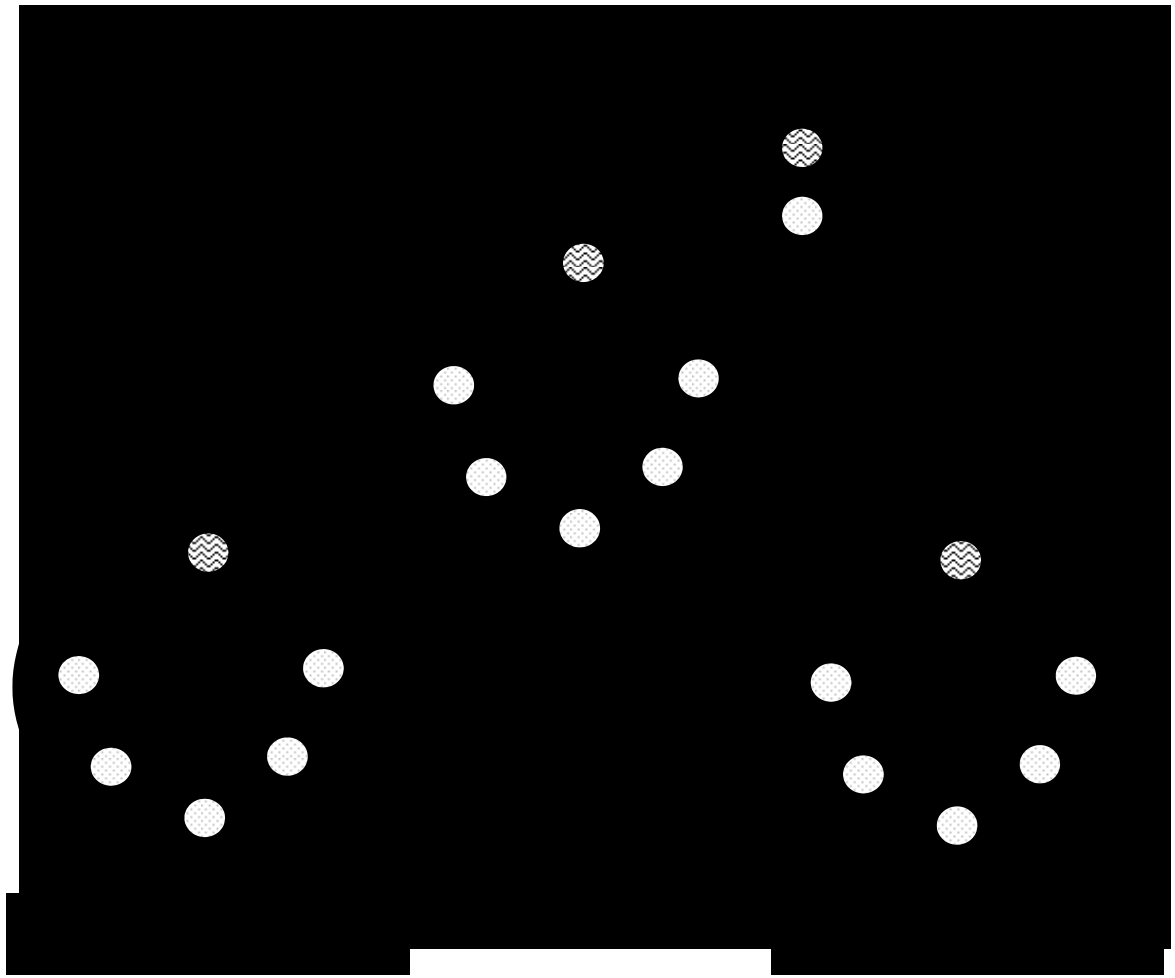
lightweight

flexible

resilient

against security threats

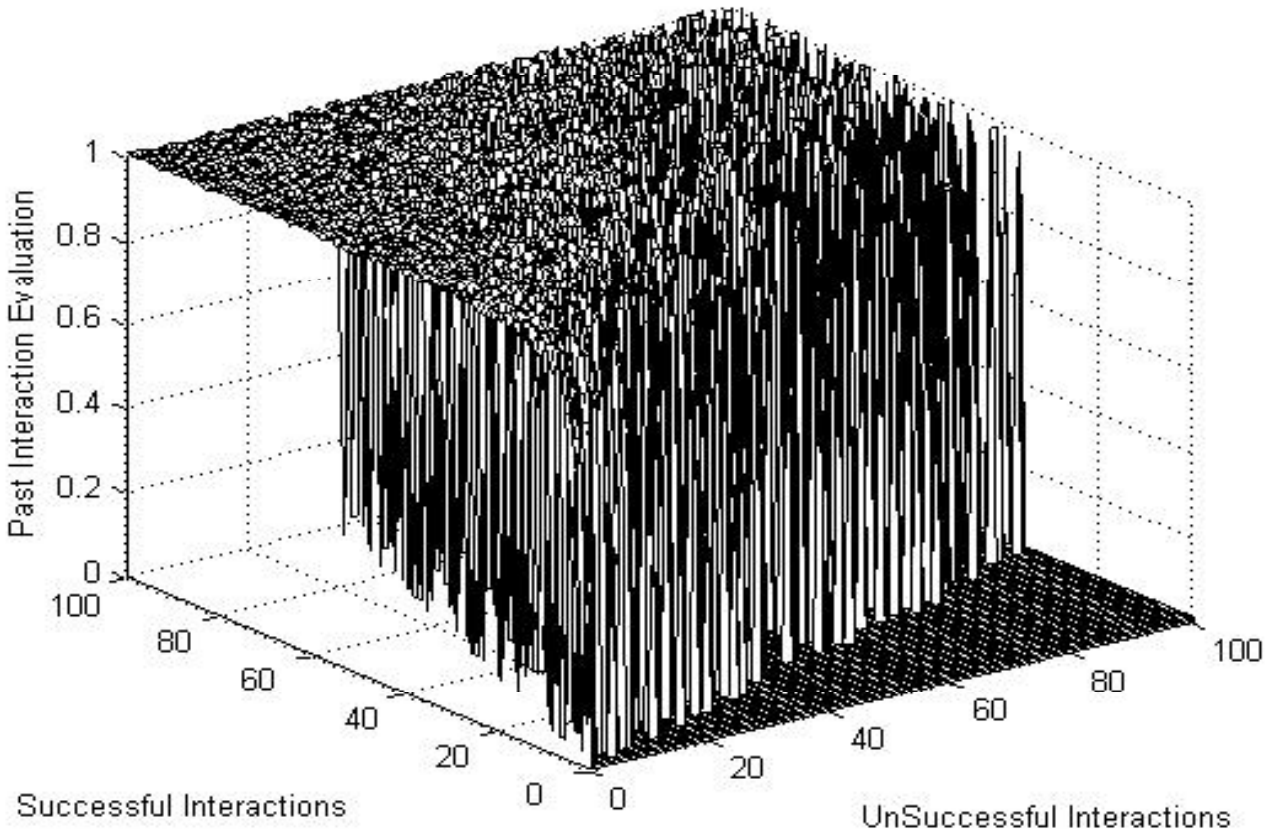
Group based Trust Management Scheme



Trust Calculation at Node Level

- At Node level, trust value is calculated by using time based past interaction as well as peer recommendations.
- Time based Past Interactions Evaluation:

Trust Calculation at Node Level (Cont…)



Trust Calculation at Node Level (Cont…)

- Peer Recommendations Evaluation:

- Formation of Trust Value:

Trust Calculation at Node Level (Cont…)

- Memory Requirement
- Each node maintains the small trust database as shown in table 1.

- The size of each record is 22 bytes. Therefore memory requirement for GTMS at each sensor node is *(n-1)*22* bytes, where n is number of nodes in the cluster

Trust Calculation at Cluster Head

- Here we assume that Cluster Head is the sensor node that has higher power and memory as compare to other sensor nodes.
- In response all group member nodes forward their trust values of other member nodes to cluster head. The trust vector of cluster head node is defined as

- Where $Tv_{ch,i}$ represent the trust of node i. It is calculated as

- This Trust vector is forwarded to BS.

Trust Calculation at Cluster Head (Cont…)

- Formation of Trust Value:

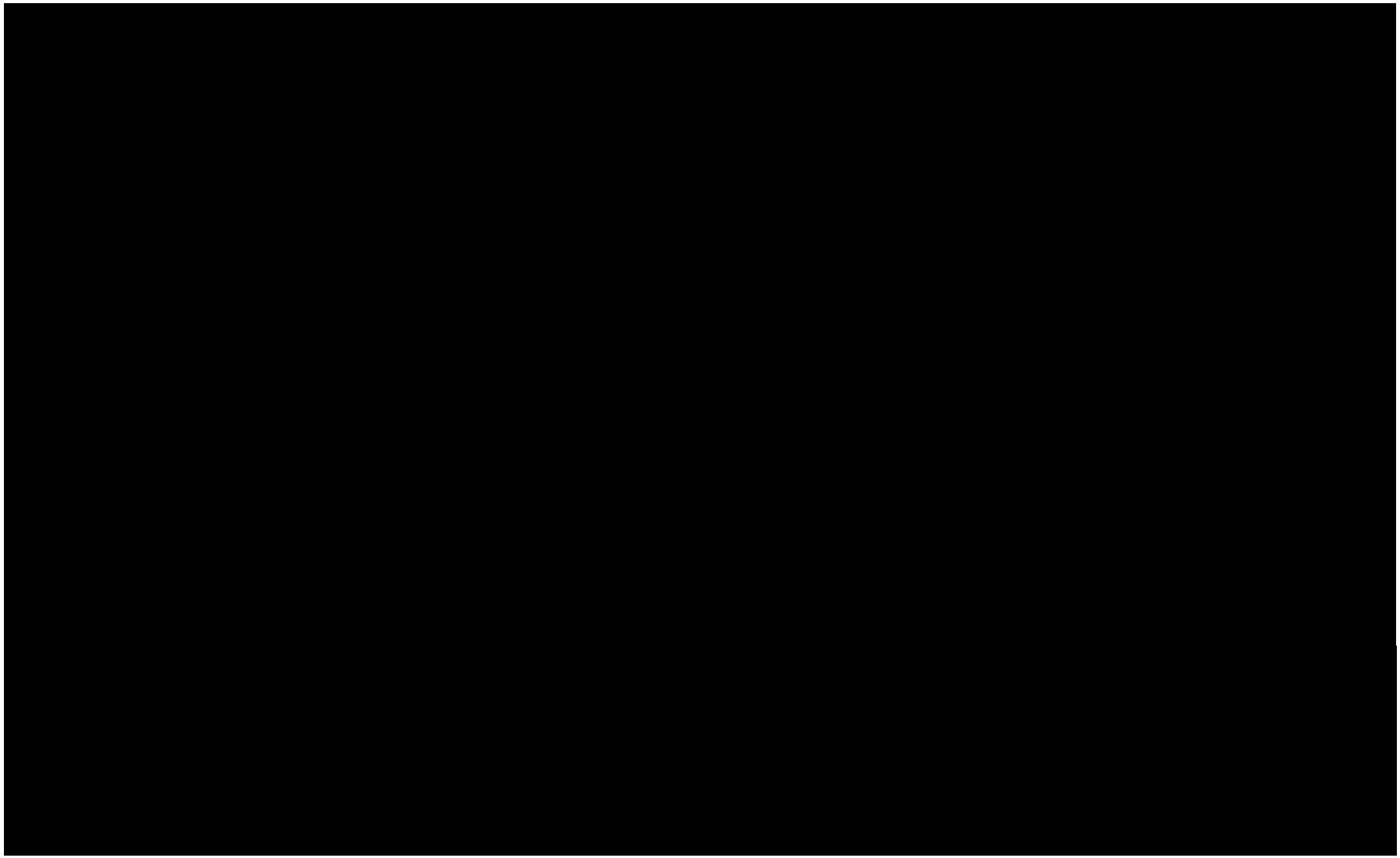
Trust Calculation at Cluster Head (Cont…)

- Cluster head maintains two databases; one is similar to individual's sensor node trust database and in second CH maintains the trust values of other groups as shown in table 2.

- The size of each record is 22 bytes. Therefore the total size of table 2 is *(m-1)*22*. Here 'm' is the total number of groups in the network.

- In order to save all trust values in both database cluster head needs *(n+m-2)*22* bytes of memory space.

Trust Calculation at Base Station



Conclusion

- Research on trust management scheme for wireless sensor networks is at very infancy state and current sensor network security solutions are based on assumption of trusted environment.
- Therefore in this work, we have proposed novel group based trust management scheme (GTMS) for distributed wireless sensor networks that is based on hybrid trust management approach.
- GTMS is very simple and flexible and doesn't require any large storage of data and complex computations at single sensor node.

Future Work

- Our work is in initial phase, Now are now in the phase of implementation of GTMS scheme that will gives us the information about computation and communication overhead.

- Our Trust model is based on the assumption that every node has a unique id but the following challenging problem is still open:

"how to assign identities and trust values to sensor nodes in a large scale anonymous environment where nodes have no unique id?"

Suggestions and Recommendations

Email: riaz@oslab.khu.ac.kr