An Overview of Key Management in Wireless Sensors Network

Akhlaq Ahmed
Liverpool Hope University
Akhlaq2000@yahoo.com

Abstract

These days wireless communication is gaining popularity. With the recent advancement in wireless industry, we became aware of a new technology know as wireless sensor network. Wireless sensor network is one of the new additions in the family of wireless network. The combination of Micro-electro-mechanical system (MEMS) and wireless communication technology makes wireless sensor networks as practical vision to deploy a large-scale, low power, inexpensive sensor networks. Wireless sensor networks guarantees advantages over the traditional sensing methods in many ways: large-scale, densely deployment not only extends the spatial coverage and achieves higher resolution, but also increases the fault-tolerance and robustness of the system, their ad hoc nature and deploy vision make it even more attractive in military applications and other risk-associated applications. Such as habitat monitoring and environmental observations. Due to the potential advantages associated with wireless sensor networks, the research in this area growing continuously. At present, research prototypes and sensor nodes are designed and manufactured. Energy efficient topology control protocols and routing schemes have been implemented and evaluated; various
enabling technologies, such as time synchronization, localization and tracking, key management are being studied and invented. The contribution of this work is to investigate the key management of the wireless sensor networks. We believe that the findings as presented in this work will be beneficial specially in designing and developing secure solution in wireless sensor networks.

1. Introduction

The development in wireless communication and electronics has enabled the manufacturing of low cost, low power, multifunctional sensor which is economically feasible. These sensors are small in size and are capable of data processing and wireless communication in short distances. Wireless sensor network is the distributed network of these tiny sensors also called the nodes, consists of sensing, data processing and communicating components leverage the idea of sensor network, these nodes are dedicated to closely observe the real world phenomena. Sensor network is made up of a large number of sensors which are thrown from an aeroplane in to an area which is under observation. This sensor doesn’t need any type of preplanning for their nodes to make a network to communicate with each other. It has self organising capabilities. When additional sensors are added or old sensors fail, the sensors re-organize themselves to take advantage of the Added system resources Akyildiz. F. I, Su. W, Sankarasubramanium. Y and Cayirci. E. (Aug 2002).

some of the key management techniques achieve some parameters from security point of view but they
are too expensive, our research shows that in wireless sensor network in such a limited resources hundred percent security solution is not possible. Therefore we need a trade-off between security and resources. By using the wireless sensor network we are able to monitor and control wide physical environment from remote location. A large number of sensor nodes make the sensor network, these nodes are separately connected to the neighbouring nodes through the wireless network and they use a multi hop routing protocol to communicate to the nodes that are far from them.

At present, research prototypes and sensor nodes are designed and manufactured. Energy efficient topology control protocols and routing schemes have been implemented and evaluated; various enabling technologies, such as time synchronization, localization and tracking, key management are being studied and invented. We have investigated the key management of the wireless sensor networks. We have carried out in depth research by collecting related materials from various resources. The findings of this work shows that some of the key management techniques achieve some parameters from security point of view but they are too expensive, our research shows that in wireless sensor network in such a limited resources hundred percent security solution is not possible. Therefore we need a trade-off between security and resources.

Rest of this paper has been organized as follows. In section 2, Related work is presented. Analysis and discussion is detailed in section 3 whilst conclusion and future is presented in section 4.
2. Related Work

Wireless sensor networks are rapidly gaining popularity because of its low cost solutions to a variety of real-world challenges. (Akyildiz. F. I et al, Aug 2002)

We are able to perform both military and civilian tasks due to their low price which provide large sensor arrays in variety of conditions. But Sensor network also has some of the resource restraints of its lack of data storage and its energy. Due to these constraints the traditional computer security techniques in wireless sensor network could not be implemented along with this the unreliable communication channel and unattended operation makes the security operations very harder.


Before the Wireless sensor network often have very low processing power and the industrial trend was only to reduce the cost of the wireless sensor with no change in the processing power. Keeping this in mind the researchers start challenging the wireless sensor with maximizing the processing capabilities and energy reserves of each sensor node while also securing them against attackers. All of the traditional security issues have been examined for the Wireless sensor network and conclude that some of the general-purpose sensor network techniques assumed that all nodes are cooperative and trustworthy. And the natural unattended feature of wireless sensor network make us disagree that the physical attacks to
sensors play an important role in the operation of wireless sensor network Walters.

Cryptographic key is one of the security mechanisms which can be used for the communication between two parties. Menezes. A., Oorschot. V. P., Vanstone. S., (1997). There is still so much to do in key management in WSN. The traditional key management techniques are not suitable for WSN due to limited resources there are two types of keying schemes wireless sensor network i.e. Key pre-distribution is the only option available to the WSN where its topology is not known before the deployment. Echenauer. L., Gligor D. V., (November 2002)

For the secure communication these keys must be installed in every sensor node. However traditional key-distribution schemes have the following shortcoming: either a single mission key or a set of separate n - 1 key, each being pairwise privately shared with another node, have to be installed in every sensor node Hu F., Sharma K. N (2003). In key pre-distribution, we have the big issue that how we can set keys also called key rings in to the limited memory of each node. Saving the key identifiers of a key that are loaded through out he network and then associating the sensor identifiers with a trusted controller node is also some of the problems.

In a wireless sensor network every node has to know about its neighbour with which a connection is established and afterwards key is shared. It is also known as shared-key discovery that establishes the topology of the sensor array. A shared key makes a link between two sensor nodes. Particularly in a sensor
node a connection is established if and only if two nodes share a key. This sharing of connection can also be termed as link. Because of this shared key between the neighbours a bond is made between one node and the other and so on. This neighbour discovery scheme will stop the attacker(s) to find out about or discover the shared key. Hence the attacker can only check, analyse and know about the network traffic.

The focus of the following section is to analyse and discuss findings in view of the above presented literature work.

3. Analysis and Discussion

Recent advances in wireless communications and electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate undeterred over short distances. These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks. Sensor networks represent a significant improvement over traditional sensors. Akyildiz, F.I., SuW., Sankarasubramaniam, Y., and Cavirci, E (2002)

Wireless Sensor Network is an exciting research area due to its constraints. The reason of WSN (Wireless Sensor Networks) popularity is because of a small size sensor, its operations, and its networking behaviour which enables it to give a lot of advantages in many applications which were not possible in the past. Battle field surveillance, forest fire detection, smart environment, and environmental control in office buildings are well known applications.
In WSN indoor and outdoor applications communications can be monitored and nodes are subjected to capture and surreptitious use by an adversary. Echenauer, L., Gligor D. V (2002). For that reason the cryptographic protected communications are required. A keying relationship is the state where in communicating entities share common data (keying material) to facilitate cryptographic techniques. This data may include public or secret keys, initialization values, and additional non-secret parameters Anna Hac, *Wireless Sensor Networks*, John Wiley & Sons, 2003.

Key management is the set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties. There are two simple strategies for Key management schemes. One is to use a single secret key over the entire network. This scheme is obviously efficient in terms of the cost of computation and memory. However the compromise of only a single node exposes all communications over the entire network, which is a serious deficiency. The other approach is to use distinct keys for all possible pairs of nodes. Then every node is preloaded with $n - 1$ key, where $n$ is the network size. This scheme guarantees perfect resiliency in that links between non compromised nodes are secure against any coalition of compromised nodes. However this scheme is not suitable for large networks since the key storage required per node increases linearly with the network size. It means in the first strategy the sharing of keys between nodes is high and in the second strategy sharing between the nodes is low.
Due to need of secure communication and limited resources researchers are proposing solutions between these two strategies.

Due to the disordered structure of WSN any proposed solutions for key management in indoor sensor networks is difficult to implement in outdoor applications. However there are good solutions for key management but when the network expands, or the structure of network changes, these methods fail. We therefore propose an efficient key management solution.

4. Conclusion and Future Work

The contribution of this work is to review key management security mechanisms in wireless sensor network. The conclusion of our research shows that some of the key management techniques achieve some parameters from security point of view but they are too expensive, our research shows that in wireless sensor network in such a limited resources hundred percent security solution is not possible. Therefore we need a trade-off between security and resources. In future we intend to contribute similar findings in the ongoing research in this field.

References


