Leap Protocol in Wireless Sensor Network

Ms. Apurva R.Raut, Mr. Sanghesh B. Bele, Ms. S. K. Totade

Department of MCA, Vidyabharati Mahavidyalaya, Amravati

ABSTRACT- Wireless sensor network are becoming significantly vital to many applications, and they were initially used by the military for surveillance purpose. One of the biggest concerns of WNS is that they are very defenseless to security threats. Due to the fact that these networks are susceptible to hackers, it is possible for one to enter and

render a network. For Example, such network may be hacked into the military, using the system to attack friendly forces, for this a key management protocol for sensor network i.e. LEAP (Localized Encryption and Authentication Protocol) is designed to support in-network processing. The design of protocol is motivated by the observation of different types of messages exchanged between sensor nodes have different security requirements and that single keying mechanism is not suitable for meeting these different security requirements , and LEAP uses four types of key for each sensor node. The prototype implementation of LEAP in sensor network is also reported.

Keywords*: Key Management (four key used by LEAP) , Sensor Network , Designing Goal of LEAP, Working of LEAP, TDMA-slot, TDMA-cycle, NS2Platform.*

INTRODUCTON

Wireless Sensor Network spatially consist of distributed autonomous sensors to monitor physical and environmental conditions such as temperature, sound, vibration, pressure motion and pollutants and to cooperatively pass their data through network to main location with the help of protocol.

Protocol: It specifies the standard for communication and provides detail information on processes involve in data transmission. A single process can handle by more than one protocol simultaneously.

LEAP (Localized Encryption and Authentication Protocol) is a proprietary wireless LAN (Local Area Network) authentication method developed by Cisco System. Important feature of LEAP is dynamic WEP (Wired Equivalent Privacy) Keys and mutual authentication between a wireless client and RADIUS (Remote Authentication Dial In User Service) Server.

LEAP (Localized Encryption and Authentication Protocol) , sometimes called EAP(Extensible Authentication Protocol)-Cisco Wireless, is interesting in that it was really the first commercial use of IEEE 802.1X and EAP(Extensible Authentication Protocol) for wireless LAN(Local Area Network)

LEAP (Localized Encryption and Authentication Protocol) PROTOCOL:

LEAP (Localized Encryption and Authentication Protocol) is the authentication protocol used in wireless network and point-to-point connection. LEAP is designed to provide more secured authentication for 802.11 WLANs (wireless local area networks) that support 802.1X port access control. It is a key management protocol for sensor network that is designed to support in-network processing, while providing security properties similar to those provided by pair wise key sharing schemes. LEAP includes support for multiple keying mechanisms. The design of this mechanism is motivated by the observation that different types of messages exchange between sensor nodes have different security requirements.

DESIGN GOAL

LEAP is designed to support secure communication in sensor network, therefore it provide the basic security services such as confidentiality and authentication. In addition LEAP is to meet several security and performance requirement that are considering more challenging to sensor network.

- Supporting Various Communication Patterns :

There are typically three types of communication pattern in sensor network : unicast (addressing a message to single node) , local broadcast (addressing a message to all the nodes in the neighborhood) , and global broadcast (addressing a message to all the nodes in the network).

- Supporting In-network Processing: Security mechanism should permit in network processing operation such as data aggregation and passive participation. In network processing could significantly reduce energy consumption in sensor network.

- Survivability: Due to the unattended nature of sensor network an attacker could launch various security attacks and even compromise sensor node without being detected. Therefore , a sensor network should be robust against security attacks, and if an attack succeed , its impact should be minimized .

- Energy Efficiency: Due to the limited battery life time, security mechanism for sensor network must be energy efficient. Especially, the no of message transmission and the number of expensive computation should be as few as possible. Moreover size of sensor should not be limited by the pre-node storage and energy resources.

- Avoiding Message Fragmentation: A unique challenge in sensor network is due to small packet size. The default supported packet size is only 36 bytes for increasing the reliability of packet delivery. Thus the message in security protocol has to be small enough to fit in one packet to avoid message fragmentation.

Key Management Scheme:

LEAP supports the establishment of four types of keys for each sensor node :

An individual key shared with the base station. Every key has unique key that it shares with the base station. This Key is used with secure communication between nodes and the base station. Individual key is used to compute message authentication code for its sensed reading by node, if it is verified by base station.

A pair wise key shared with another sensor nod:

Every node shares pair-wise key with each of its neighboring node. In LEAP pair wise key is used for securing communication that requires privacy and source authentication. Each node can used its pair-wise key to secure the distribution of cluster key to its neighbor or to secure the transmission of its sensor reading to an aggregation node.

A cluster key shared with multiple neighboring nodes:

A cluster key is key shared by node and its neighbors and it is mainly used for securing locally broadcast message i. e. routing control information or securing sensor messages which can benefit from passive participation.

A group key shared by all nodes in the network:

This is globally shared key used that is used by base station for encrypting message that are broadcast to the whole group. For Ex: The base station issues missions , send queries and interests.

Security Requirements for Key Management

To provide secured communication in WSN, sensor node first need to setup pair-wise with each other. There are some majors:

Data Confidentiality: In sensor network data flows from many intermediate nodes and chances of data leak is more hence only encrypted data is used so that only recipient decrypts the data to its original form.

Data Integrity: Data receive by receiver should not be altered or modified is data integrity.

Data Authentication: It is the procedure for confirmation that the communicating nodes is the one that it claims to be. It is important for receiver to do verification that the data is receive from authenticate node.

Data Availability: This means the services are available all the time even in case of some attacks such as Denial of service.

Source Localization: For Data transmission some application use location information of the sink node. It is important to give security to the location information. Non-secured data can be controlled by the malicious node by sending false signal strength or replaying signals.

Self-Organization: In WNS no fixed infrastructure exists , hence every node is independent having properties of adaption to the different situation and maintain self organizing and self healing properties. This is the great challenge for security in WNS.

Working of LEAP

The process is summarized as:

1. The authentication server challenges the device by sending a random string. The device must prove it knows the key by sending response derived from challenge.
2. The device sends a challenge to the authentication server, which must also respond correctly.
3. The authentication server generates and sends a session key to access point with the EAP (Extensible Authentication Protocol) success notification in RADIUS (Remote Authentication Dial In User Service) message.
4. The access point notifies the device of authentication using the EAPOL (Extensible Authentication Protocol Over LAN)-Success message. At this point the client computes the matching session key.
5. The access point sends an EAPOL(Extensible Authentication Protocol Over LAN) key to activate encryption.
6. The device and access point communicate using WEP encryption.

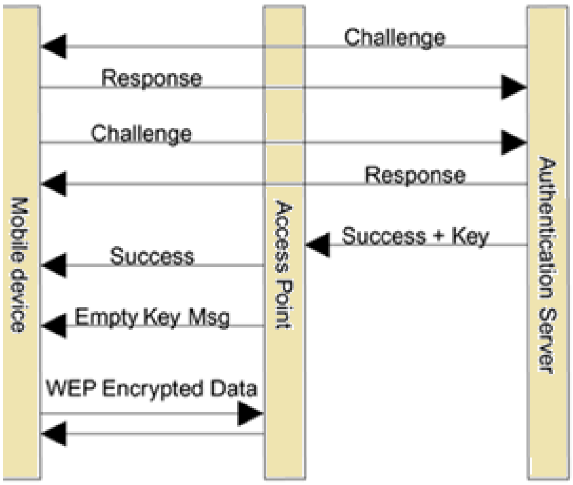

Figure 1: EAP-LEAP

Hardware Technologies

A sensor network is an embedded system, or rather a digital system committed to specific duties. Each node consist of sensor board and a programming board. The sensor board could be differentiating by specific kind of sensor. Light, temperature, humidity but also distance tracking or GPS receiver. The programming board supplies wireless between a node and a base station. A node is equipped with a microcontroller and low storage memories.

NS2 Platform : It is an open source simulation tool that runs on LINUX . It is a node platform for low power and high data rate sensor network applications designed with dual goal of fault tolerance and development ease. The low power operation of the module is due to the low power T1 MSP430 microcontroller. This 16-bit RISC processor features low active and sleep current consumption. In order to minimize power consumption, the processor in sleep during majority of the time , wakes up s fast as possible to process , then return to sleep mode again.

Software Technologies

It follows the demand of specific ad hoc software technologies. Hence, operating system for WSN nodes are typically less complex than general-purpose operating system. In general operating system in WSN should fulfill requirements like:

1. Robustness: once deployed, a sensor network must work unattended for months and years.
2. Low resource usage: sensor network node includes very small RAM, and run off batteries.
3. Multiple service implementations: application should be able to choose between various implementations.
4. Adaptability to evaluations: mote hardware is in constant evaluation, application and most system service must be portable across hardware generation.
5. Adaptability to application requirements: applications have very different requirements in terms of life time, communication, sensing etc.

Leap implement token passing procedure that:

- Ensures synchronization between nodes and clusters.
- Allows initializing and self configuring to the optimal working point
- Allows for the addition of new nodes

A token is a particular message that carries the information on the duration of TDMA-slot and a TDMA-cycle, the transmitting and receiving schedule of TDMA-cycle, a synchronization message carrying the current execution state of the TDMA-cycle. The controller has all the information to calculate the optimal set of parameters, consequently, it is able to generate a token before the network starts operating. The network initialization algorithm works as :

1. When the network starts all nodes are awake and listening.
2. The controller multi cast the token to all nodes of one of the connected cluster.
3. Nodes of the selected cluster read the information on scheduling and duration of TDMA-slot and TDMA-cycle. Moreover each node acquires the information about the global time and launches periodic timer for CSMA and TDMA slot. In the midtime, a random back-off timer starts for each node before sending an acknowledgement.
4. The first node that expires the back-off time sends the acknowledgement to the controller and become the token forwarder. Then all nodes in the cluster go to sleep.
5. At the beginning of the second TDMA-slot the token forwarder wake up and immediately multi-casts the token to all nodes in the next cluster.
6. With the same random acknowledgement-based scheme, a node is elected token forwarder for nodes in following cluster.
7. Information about routing and TDMA-slot duration needs also to be updated during network operation. Hence, the Controller periodically performs a token refreshing procedure.

Conclusion

The LEAP protocol was implemented and simulated using one base station and fifty sensor nodes situated randomly. Initially, an individual key was generated for each node from a randomly generated master key. Then a cluster key was generated by each node and published to their neighboring nodes using the pair –wise keys. Finally the global key was generated in order to enable public broadcasts.

The whole idea behind LEAP was to implement a system whereby multiple base station have been employed for the soul purpose of improving tha data transmission amongst node and to come up with a solution for base station , should it be compromised.

References

1. A Semi Random Protocol Solution for Clustered by A. Bonivento, C. Fischione, A. Sangiovanni-Vincentelli.
2. Burgner, D. E. & Wahsheh. L. A. Security of wireless sensor network ,Eighth International Conference on I.T.
3. Network Security And Essential by Williams 4th Edition PDF
4. “LEAP” Efficient security mechanism for larger scale distributed sensor network -1oth ACM Conference on computer and communication security.
5. A Time-Based Key Management Protocol for WNS – Jiyong Jang ,Sejong University
6. Security in wireless sensor network improving the LEAP protocol –Delan Alsoufi, Khaled Elleithy ,University of Bridgeport, International Journal of computer science & engineering Vol3,2012 June
7. http://www.mpirical.com/glossary/leap-lightweight-extensible-authentication-protocol.
8. http://www.etutorials.org/Networking/802.11+security....+Cisco +Light+EAP+LEAP/