INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

CONFIDENTIAL DATA DISCOVERY AND DISSIMINATION USING AODV PROTOCOL

[1]P. RUBA, [2]R.A. ROSLINE M.Sc., M.Phil.

[1]Department of Computer Science, Government Arts College, Coimbatore -18.
[2]Assistant Professor, Department Of Computer Science, Government Arts College, Coimbatore -18
E-mail:Rubashree.15@gmail.com, E-mail: roselinera@yahoo.com

Abstract

As a Wireless Body Area Networks (WBANs) are emerging as important in various fields. Wireless body area network consists of multiple sensor nodes, these sensors are placed strategically on human body as tiny patches allowing ubiquitous health monitoring in their native environment for extended period of time. After WBAN is deployed, it is sometimes necessary to confidential data into the network through wireless links to Adjust configuration parameters of body sensors. Multi-key cryptography is the study of mathematical techniques. It is related to aspects of information security such as confidentiality, data integrity, entity authentication and origin authentication. Based on multiple one-way multi-key hash chains, our protocol provides frequent authentication and can tolerate node compromise. This paper reports the experimental evaluation of AODV protocol in a network of resource limited sensor nodes, which shows its efficiency in practice. In particular extensive security analysis shows that AODV protocol is provably secure.

1. OVERVIEW OF WIRELESS BODY AREA NETWORK

A Wireless Body Area Networks (WBAN) is the network that permits the combination of smart, small scale, minimum power, aggressive/discreet sensor nodes which monitors body activities and neighboring environment. Every intelligent node in the network has potential to forward the information to the base station after processing to obtain the diagnosis and prescription .The application of WBANs is concerned with medical field and it also upholds consumer electronics applications concurrently. A Wireless Sensor Networks (WSNs) consist of a large number of nodes with sensing, computation, and wireless communication capability. These sensor networks are typically deployed to collect data from the environment or other physical spaces.

In an operational WSN (including WBAN), some common variables may be stored in each node of the network. The data discovery protocols add, delete, and modify such variables by requesting each node to exchange packets so that they eventually become consistent across the network. In the literature, a number of data discovery and dissemination protocols have been proposed. The proposed protocols focus on reliable data dissemination but ignore the security aspect. Thus, ensuring security in these protocols is an unresolved issue.

The problem of secure data discovery and dissemination for WBANs, we need to take into account the distinct features of WBANs. For example, all existing security solutions which involve cryptographically strong protocols incur too much computation and communications cost for body sensors. Each node needs to broadcast new data. Adversaries can easily exploit this feature by launching DOS attacks to drain the resources of body sensor nodes from their intended functions.

Motivated by the aforementioned observations, this paper has the following main contributions:

1) We first investigate the security issues in data discovery and dissemination protocols for WBANs and point out that there is a need of authenticating the disseminated data.

2) The unique features of a WBAN, we extend Drip to become a secure, lightweight, confidential, and denial-of-service (DOS)-resistant data discovery and dissemination protocol for WBANs based on the use of multiple one-way key hash chains. We demonstrate that our protocol incurs lower computational, energy and communication costs while securing the multi-hop dissemination of data items. Also, we apply the provable security technique to formally prove the authenticity and integrity of the disseminated data items in our protocol.

3) We implement our proposed protocol AODV (Adhoc on-demand distance vector Routing) Measurements from experiments verifies its high efficiency in practice.

2. METHODS OF CONFIDENTIAL DATA DISCOVERY

The main methods of confidential data discovery can be divided into following groups

2.1 Confidential Data Discovery for Security Vulnerabilities:

WBANs may be subject to malicious attacks from external attackers. By placing an intruder node or compromising a node of the WBAN, an adversary could possibly modify or replace the legitimate data being propagated in the WBAN. Furthermore, an adversary can reboot the whole network with wrong data data* by injecting a fake data item (key, version, data*) to the network where version is larger than all version numbers of the concerned variable stored on the body sensor nodes. Alternatively, the adversary can even erase an important variable identified by key from all sensor nodes by sending the data item (key, version, 0) using a data discovery and dissemination protocol, where version is a large enough number.

Each data item contains a unique key to identify the variable (i.e., parameter or command) that it aims to update, and a value to reflect its freshness. In Drip, each data item is formatted as a three-tuple (key, version, data), in which key identifies uniquely the concerned variable, version indicates whether the data item is new (a larger version means a newer data), and data denotes the disseminated value for the concerned variable.

2.2 Multi-key Generation:

The development of multiple key cryptography technique has a long and fascinating history. Such development dramatically accelerated, which some believe is largely due to the globalization process. multiple one-way hash chains to secure the proposed protocols. Hash chains are based on a function H (.) with the property that its computation is easy, whereas its inverse H−1 (.) is extremely difficult to compute. A hash chain with length b is generated by applying H (.) to an initial element repeatedly for b times. The last value after H (.) has been applied b times is called the committed value of the hash chain.

2.3. Hash Function

Hash chains are based on a function H(.) with the property that its computation is easy, whereas its inverse H−1 (.) is extremely difficult to compute. A hash chain with length b is generated by applying H(.) to an initial element repeatedly for b times. The last value after H(.) has been applied b times is called the committed value of the hash chain.

The nodes are deployed the base station constructs N hash chains as follows. It generates N distinct random seed numbers and computes a one-way hash chain with the length b starting from each seed, the (b –i)th output of hash function derived from the j th random seed number (i.e., Kb,j) is denoted as Ki,j. Here, the length b of each chain can be arbitrary but no less than the number of data items that the base station wants to disseminate in the lifetime of the network.

3. PROTOCOL CHALLENGES

To satisfy the confidentiality and authenticity requirements, the protocol that implements the Send access control primitive discussed above needs to authenticate the sender in a confidential manner.

3.1 Ad hoc on-demand Distance Vector (AODV) Routing Protocol

AODV is an improvement on DSR (Dynamic Source Routing) because it typically minimizes the number of required broadcasts by creating routes on a demand basis. AODV routing protocol uses reactive approach for finding routes, that is, a route is established only when it is required by any source node to transmit data packets. The protocol uses destination sequence numbers to identify the recent path. In this protocol, source node and the intermediate nodes store the next node information corresponding to each data packet transmission. In an on-demand routing protocol, the source node floods the Route REQuest (RREQ) packet in the network when a route is not available for the desired destination. It may obtain multiple routes to different destinations from a single RREQ. A node updates its path information only if the destination sequence number of the current packet received is greater than the last destination sequence number stored at the node. A RREQ carries the source identifier (SrcID), the destination identifier(DestID), the source sequence number (SrcSeqNum) and destination sequence number (DestSeqNum), the broadcast identifier (BcastID), and the time to live (TTL) field. DestSeqNum shows the freshness of the route that is selected by the source node. When an intermediate node receives a RREQ, it either forwards it or prepares a route reply (RREP) if it has a valid route to the destination. The validity of a route at the intermediate node is determined by comparing the sequence number at packet. If a RREQ is received multiple times, which is indicated by BcastID-SrcID pair, then the duplicate copies are discarded. All intermediate nodes having valid routes to the destination, or the destination node itself are allowed to send RREP packets to the source. Every intermediate node, while forwarding a RREQ, enters the previous node address and it BcastID. A timer is used to delete this entry in case a RREP is not received before the timer expires. This helps in storing an active path at the intermediate node as AODV does not employ source routing of the data packets. When a node receives a RREP packet, information about the previous node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop towards the destination.

In our protocol, symmetric key cryptography is used to achieve data confidentiality because they are computationally efficient even for resource constrained body sensor nodes. To prevent the untrusted nodes to forge the broadcast data items, the symmetric keys are changed on a per-packet basis. The symmetric keys are derived from a one-way hash chain, where a key can only be verified, but cannot be forged, from the previous key. Therefore, the authenticity of the broadcast data items is achieved. Our protocol generates different key chains for nodes in different hop groups. More specifically, the base station establishes multiple distinct one-way key chains, each of which corresponds to the nodes with the same hop distance from the base station.

4. EVALUATION RESULTS

The simulation experiment was performed on a computer with Intel core 2 Duo 1.7 GHz processor and 2GB RAM. The simulation experiment was performed twice by taking 50 and 100 node to study the effects of the three attacks by measuring the performance of the network. In each of the case i.e. 50 nodes and 100 nodes simulation was carried out several times with different seed values.

The performance of the network was evaluated by using the following four metrics (i) Packet Delivery Fraction (PDF), (ii) Average End-to-End Delay, (iii) Throughput and (iv) Routeerror.

Packet Delivery Fraction (PDF): It is a ratio of the data packets delivered to the destinations to those generated by the Constant Bit Rate (CBR) sources.
Average End-to-End Delay: This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.
Throughput: It is equal to the average performance of all nodes duringsimulation. It is a calculation of bits per second processed by each node.
Route Errors: The error messages garneted by the protocol during simulation.

Simulation was performed by taking different seed values. In the experiment, the numbers of malicious node were increased starting from 5% to maximum of 30 % in the step of 5%. The Glomosim simulator generated a GLOMO.STAT file which contained all the statistics regarding number of packets send, number of packets received, number of bytes sent, number of bytes received, throughput(bits per second), delay (in seconds), number of route errors etc.

5. CONCLUSION

The security mechanisms that the protocol uses are the hash chain, digital signature and Protocol Enforcement Mechanism. It uses low complexity symmetric cryptographic techniques for maintaining confidentiality. The performance of the protocol (AODV) was tested in simulation and their communication costs were measured using the NS-2 simulator, which was suitable for the present purpose. The evaluation metrics used in this study were overhead and end to end delay, both the cases our protocol show better performance.

REFERENCES

[1] G.Tolle and D.Culler, "Design of an application-cooperative management system for wireless sensor networks," in Proc. Eur. Conf. Wireless SensorNetw., 2005, pp. 121–132.
[2] K. Lin and P. Levis, "Data discovery and dissemination with DIP," in Proc. ACM/IEEE Int. Conf. Inform. Process Sensor Netw, 2008, pp. 433–444.
[3] T. Dang, N. Bulusu, W. Feng, and S. Park, "DHV: A code consistency maintenance protocol for multi-hop wireless sensor networks," in Proc.Eur. Conf. Wireless Sensor Netw., 2009, pp. 327–342.
[4] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen, "Distributed access control with privacy support in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 10, no. 10, pp. 3472–3481, Oct. 2011.
[5] D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks," IEEETrans. Wireless Commun, vol. 12, no. 9, pp. 4638–4646, Sep. 2013.
[6] Z. Zhang, H. Wang, A. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," IEEE Trans. Inf. Technol. Biomed., vol. 16, no. 6, pp. 1070–1078, Nov. 2012.