International Journal of Computer Science and Engineering Communications,
Volume.4, Issue.2 (2016): Page.1384-1387
www.scientistlink.com/ijcsec

Safe and Distributed Data Sharing in Wireless Sensor Network by Using Revocation Process

A. Sasikala[1], K. Kumaresan[2]
PG Scholar[1], Assistant Professor[2]
Department of Computer Science and Engineering,
K.S.R College of Engineering, Tiruchengode, India
sasianju757@gmail.com[1], kkumaresanphd@gmail.com[2]

Abstract: *Distributed data discovery and dissemination protocol for wireless sensor networks is responsible for allows the network owners to authorize multiple network users with different privileges to simultaneously and directly disseminate data items to the sensor nodes. In existing protocols suffer from two major drawbacks present in wireless network. First they are based only security in network not safety in sensor nodes. Second those protocols are not designed with security in mind and thus adversaries will simply launch attacks to damage the data packets. This paper proposes proving the authentication and enhancing the validation system by using revocation process. The proposed scheme also solves the improper certificate revocation which can occur due to false accusations made by malicious node also the problem of window of opportunity where revoked certificates get assigned as a valid to new nodes.*

Keywords: *certificate Authority, certificate revocation, Dissemination, efficiency, security.*

1. INTRODUCTION

A wireless sensor network is expected to consist of a potentially large number of low-cost, low-power, and multifunctional sensor nodes that communicate over short distances through wireless links. Due to the potential to provide fine-grained sensing and actuation at a reasonable cost, wireless sensor networks are considered ideal candidates for a wide range of applications, such as industry monitoring and military operations. Sometimes it is desirable necessary to reprogram sensor nodes. The wireless links after they are deployed, due to, for example, the need of removing bugs and adding new functionalities. More importantly, all existing data discovery and dissemination protocols [3], [4], [5] data items can only be disseminated by the base station. Even worse, some WSNs do not have any base station at all. For example, for a WSN monitoring human trafficking in a country's border or a WSN deployed in a remote area to monitor illicit crop cultivation, a base station becomes an attractive target to be attacked. For conventional networks, CA issue CRLs [8] which contains information about revoked certificates at regular intervals. The CRLs are either placed in online repositories where they are readily available, or they may be broadcast to the individual nodes. Alternatively, different certificate validation protocols are used for conventional network that are online certificate status protocol (OCSP), CRLs. OCSP [9] can be used to ascertain information about the status of certificate. In contrast to DICTATE [10], the proposed scheme revokes certificate of accused node only, not the certificate of accuser. Then malicious nodes can wrongfully accuse other nodes of misbehaviour and because the certificates of good, uncompromised nodes to be revoked [2]. The proposed scheme **Certificate Revocation [1]** is able to solve false accusation attack. The revocation process is security technique and this proposed protocol, the nodes which are having valid certificate only those nodes are allowed to enter into a network. The proposed scheme also solves the improper certificate revocation which can occur due to false accusations made by malicious node also the problem of window of opportunity [1] where revoked certificates get assigned as a valid to new nodes.

2. RELATED WORK

Several Recent works have attempted to provide Claude Crêpeau and Carlton R. Davis," A Certificate Revocation Scheme for Wireless Ad Hoc Networks "School of Computer Science, McGill University, Montreal, QC, Canada H3A 2A7[2]. Secure code dissemination for wireless sensor networks. The design, development, and evaluation of an efficient, secure, robust, and DoS-resistant code dissemination system named *Seluge* for wireless sensor networks. It inherits the efficiency and robustness properties from Deluge, and at the same time provides security protections for code dissemination. Deluge is an open source code dissemination system for wireless sensor networks running Tiny OS. Deluge uses a page-by-page dissemination strategy. Lanigan et al. proposed a protocol named Sluice to integrate signature and cryptographic hash

functions to provide efficient authentication for code dissemination. Deng et al. proposed a scheme to improve the DoS resilience of secure code dissemination by using Merkle hash tree. Another critical issue common to these approaches is the vulnerability to DoS attacks against the signatures used to bootstrap secure code dissemination. As a result, the adversary can broadcast packets with bogus signatures, and force all the receivers to perform expensive signature verifications. The adversary has sufficient time to launch DoS attacks against many sensor nodes.

.

3. DIDRIP PROTOCAL

DiDrip consists of four phases, system initialization, user joining, and packet pre-processing and packet verification. For our basic protocol, in system initialization phase, the network owner creates its public and private keys, and then loads the public parameters on each node before the network deployment. In the user joining phase, a user gets the dissemination privilege through registering to the network owner. In packet pre-processing phase, if a user enters the network and wants to disseminate some data items, he/she will need to construct the data dissemination packets and then send them to the nodes. In the packet verification phase, a node verifies each received packet. If the result is positive, it updates the data according to the received packet.

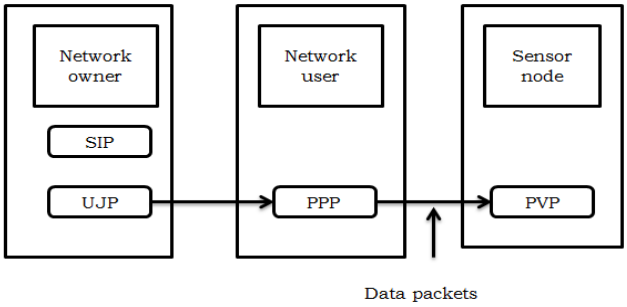


Fig.1 Information Processing Flow In DiDrip

4. CERTIFICATE REVOCATION

The proposed certificate revocation protocol for sensor networks provides a measure protection against false accusation attacks. It solves the issue of certificate revocation without taking any input from external entities. In this protocol, all trust management and key management tasks such as storage of certificate, validation of certificate and certificate revocation are performed on the individual nodes which are present within network except issuing of certificate. Information that are used to decide whether the certificate of node should be revoked or not, that information is shared by all the nodes. This will indicate that, the responsibility is given to individual node for certificate revocation and also for maintaining information about the status of the certificates of the peers with which they are communicating. So the certificate status information gets readily available towards each node; which will help to remove the window of opportunity problem. The proposed scheme also solves the improper certificate revocation which can occur due to false accusations made by malicious node also the problem of window of opportunity where revoked certificates get assigned as a valid to new nodes Voting Based Scheme [9]. This module is used to revoke the certificate of the node that has been detected as an adversary. It makes use of the information present in the PT and constructs ST from it.In this proposed certificate revocation protocol scheme, two main tables are get maintained by each and every node present in the network that are profile table (PT) shown on Table 1 and status table (ST) respectively.

Profile Table: The PT gives information about the adversary node. It also maintains information about the behavior profile of each node in the network. Information in this table is used to determine whether the certificate of node is revoked or not.

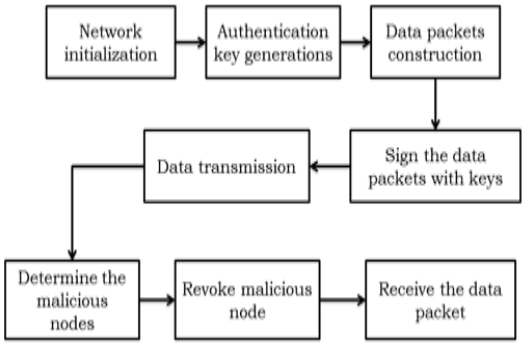
Status Table: The ST is used to find out the status of a certificate. In addition to PT, each node in the network is required to compile and maintain a ST. Initially, it is compiled from the data present in the PT, and updated simultaneously when a new accusation message is broadcasted by any node.

4.1 Certificate Acquisition and Certificate Storing

In the proposed scheme, the individual nodes within a network are responsible for all key management tasks such as certificate storing, assigning key pair to nodes, revoking certificate, except issuing of certificate due to the absence of central repositories and infrastructure support. The nodes in the WSNs need to be equipped with all aspect of network functionalities, such as routing, relaying packets etc thus the individual nodes in network is responsible for all key

management task. The certificate gets issued by a CA trusted by other network peers. A node is required to have a valid certificate issued by a CA before entering into a network. All the nodes present in network have valid certificate initially because after some period of time if it get detected as an adversary node then certificate of that node get revoked to protect the network. This module is used to issue the certificate to the nodes and store the certificate of all the nodes.

4.2 System Architecture



4.3 Requests for PT

When any new node gets entered into the network then that node required to perform 2 things that are first job which the newly entered node is required to perform is: Broadcast its certificate to all the nodes which are present in the network: The newly entered node is required to broadcast its certificate to all other nodes which are already present in the network so that the nodes already present in network obtain the information about it. Send Request to all the nodes present in the network to send their PT: The newly entered node also required to simultaneously send request to all the nodes in the network to send their PT to obtain information about the nodes that has been detected as adversary before this new node has entered into the network. Using this information the newly entered node is able to send and receive data only form non-adversary node thus the network gets protected from adversary node. In existing systems the drip and dhv protocols are used to classify network, trust and adversary models. Most importantly this protocol is not evaluate throughput, propagation delay, and energy overhead. Some time that protocols discuss their security weakness. So take that protocols are not worthy for apply the distribution and normalization function. Those protocols are less used function. It doesn't give the big difference in the security and more efficient. The proposed protocols is used to evaluate didrip; memory overhead, execution time of cryptographic operations and propagation delay, and energy overhead.

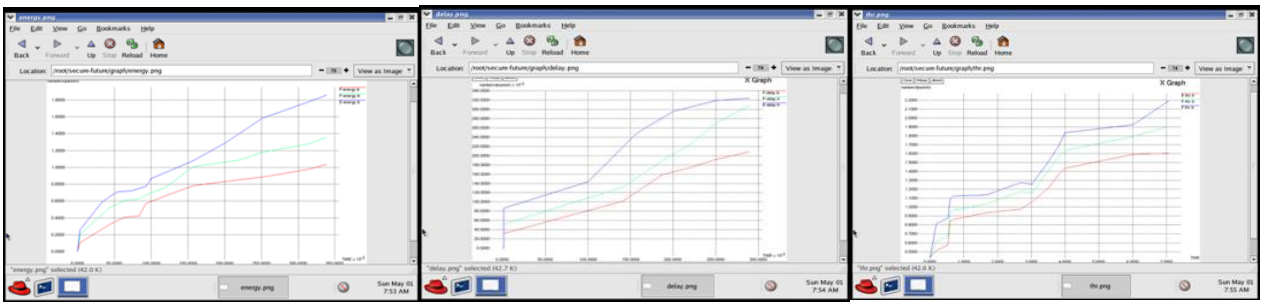


Fig.2. comparison of energy consumption. Fig.3. comparison of propagation delay. Fig.4. comparison of execution time

5. FUTURE WORK

Thus, in the future work, we will consider how to ensure data confidentiality in the design of secure and distributed data discovery and dissemination protocols. Proposed scheme, try to remove the malicious node from the network as soon as it have detected the first misbehavior of node so the time required to revoke the certificate of malicious node is get reduced compare to the time which is required to revoke the certificate of malicious node.

6. CONCLUSION

In conclusion, identifies the security vulnerabilities in data discovery and dissemination used in WSNs, which have not been addressed in previous research. Also, none of those approaches support distributed operation. Therefore, in this paper, a secure and distributed data discovery and dissemination protocol named DiDrip has been proposed. Besides analyzing the security of DiDrip, this paper has also reported the evaluation results of DiDrip in an experimental network of resource-limited sensor nodes, which shows that DiDrip is feasible in practice. We have also given a formal proof of the authenticity and integrity of the disseminated data items in DiDrip. Also, due to the open nature of wireless channels, messages can be easily intercepted. In additionally, the proposed scheme Certificate Revocation is able to solve false accusation attack .The revocation process is security technique and this proposed protocol Thus, in the future work, we will consider how to ensure data confidentiality in the design of secure and distributed data discovery and dissemination protocols. In this paper propose the sensor network security schemes utilizing threshold cryptography, potentially provide greater flexibility and security. However, the computational cost, particularly for low-powered wireless nodes, might be too prohibitive. In addition, these schemes require unselfish cooperation of the communicating peers, which cannot be guaranteed in certain networks environments. This paper proposed certificate revocation scheme for ad hoc networks, which provided some measures of protection against malicious accusation succeeding in causing the revocation of certificates of well-behaving nodes.

REFERENCES

[1] Wei Liu, Hiroki Nishiyama, N. Ansari, N.Kato, "A study on Certificate Revocation in Mobile Ad Hoc Networks", IEEE 2011.
[2] Claude Crêpeau and Carlton R. Davis," A Certificate Revocation Scheme for Wireless Ad Hoc Networks "School of Computer Science, McGill University, Montreal, QC, Canada H3A 2A7.
[3] T.Dang,N. Bulusu,W. Feng, and S. Park, "DHV:Acode consistency maintenance protocol for multi-hop wireless sensor networks," in Proc. 6th Eur. Conf.Wireless Sensor Netw., 2009, pp. 327–342.
[4] G. Tolle and D. Culler, "Design of an application-cooperative management system for wireless sensor networks," in Proc. Eur. Conf. Wireless Sensor Netw., 2005, pp. 121–132.
[5] K. Lin and P. Levis, "Data discovery and dissemination with DIP," in Proc. ACM/IEEE Int. Conf. Inf. Process. Sensor Netw., 2008, pp. 433–444
[6]K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate revocation to cope with false accusations in mobile ad hoc networks," Proc. 2010 IEEE 71st Vehicular Technology Conference: VTC2010-Spring, Taipei, Taiwan, May 16-19, 2010
[7]G. Arboit, C. Crepeau, C. R. Davis, and M. Maheswaran, "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks," Ad Ho Network, vol. 6, no. 1, pp. 17-31, Jan. 2008.
[8] R. Housley, W. Polk, W. Ford, D. Solo, Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile, Internet Request for Comments (RFC 3280), April 2002.
[9] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, X.509 internet public key infrastructure online certificate status protocol – OCSP, Internet Request for Comments (RFC 2560), June 1999.
[10] J. Luo, J. P. Hubaux and P. T. Eugster, "DICTATE: DIstributed CerTification Authority with probabilistic frEshness for ad hoc networks," IEEE Trans. Dependable and Secure Computing, vol. 2, no. 4,pp.311-323,Oct.-Dec.2005