ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

DISTRIBUTED AND PUZZLE BASED AUTHENTICATION FOR DATA DISSIMINATION IN WSN

GOBINATH.P.A,NANDHAKUMAR.J,ELANGOVAN.P
gobichena@gmail.com,nandhukvpkings@gmail.com,nsv8344547648@gmail.com
GUIDE NAME: Mr.S.SENTHILNATHAN AP/CSE
s.senthilnathan4@gmail.com

ABSTRACT

A data discovery and dissemination protocol for wireless sensor networks (WSNs) is responsible for updating configuration parameters of, and distributing management commands to, the sensor nodes. All existing data discovery and dissemination protocols suffer from two drawbacks. First, they are based on the centralized approach; only the base station can distribute data items. Such an approach is not suitable for emergent multi-owner-multi-user WSNs. Second, those protocols were not designed with security in mind and hence adversaries can easily launch attacks to harm the network. This paper proposes the first secure and distributed data discovery and dissemination protocol named DiDrip. It allows the network owners to authorize multiple network users with different privileges to simultaneously and directly disseminate data items to the sensor nodes. Moreover, as demonstrated by our theoretical analysis, it addresses a number of possible security vulnerabilities that we have identified. Extensive security analysis show DiDrip is provably secure. To improve the data confidentiality we propose Puzzling approach in wireless sensor nodes. It identifies misbehaving intermediate nodes or cluster heads and eliminates from the data transmission path.

INTRDOUCTION TO DOMAIN

A basic understanding of computer networks is requisite in order to understand the principles of network security. In this section, we'll cover some of the foundations of computer networking, then move on to an overview of some popular networks. Following that, we'll take a more in-depth look at TCP/IP, the network protocol suite that is used to run the Internet and many intranets.

Once we've covered this, we'll go back and discuss some of the threats that managers and administrators of computer networks need to confront, and then some tools that can be used to reduce the exposure to the risks of network computing.

The networks are computer networks, both public and private, that are used every day to conduct transactions and communications among businesses, government agencies and individuals. The networks are comprised of "nodes", which are "client" terminals (individual user PCs) and one or more "servers" and/or "host" computers. They are linked by communication systems, some of which might be private, such as within a company, and others which might be open to public access. The obvious example of a network system that is open to public access is the Internet, but many private networks also utilize publicly-accessible communications. Today, most companies' host computers can be accessed by their employees whether in their offices over a private communications network, or from their homes or hotel rooms while on the road through normal telephone lines.

Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

requires identifying threats and then choosing the most effective set of tools to combat them.

✓ **Threats to network security include:**
Viruses : Computer programs written by devious programmers and designed to replicate themselves and infect computers when triggered by a specific event
Trojan horse programs : Delivery vehicles for destructive code, which appear to be harmless or useful software programs such as games
Vandals : Software applications or applets that cause destruction
Attacks : Including reconnaissance attacks (information-gathering activities to collect data that is later used to compromise networks); access attacks (which exploit network vulnerabilities in order to gain entry to e-mail, databases, or the corporate network); and denial-of-service attacks (which prevent access to part or all of a computer system)
Data interception : Involves eavesdropping on communications or altering data packets being transmitted
Social engineering : Obtaining confidential network security information through nontechnical means, such as posing as a technical support person and asking for people's passwords

✓ **Network security tools include:**
Antivirus software packages : These packages counter most virus threats if regularly updated and correctly maintained.
Secure network in frastructure : Switches and routers have hardware and software features that support secure connectivity, perimeter security, intrusion protection, identity services, and security management.
Dedicated network security hardware and software- Tools such as firewalls and intrusion detection systems provide protection for all areas of the network and enable secure connections.
Virtual private networks : These networks provide access control and data encryption between two different computers on a network. This allows remote workers to connect to the network without the risk of a hacker or thief intercepting data.
Identity services: These services help to identify users and control their activities and transactions on the network. Services include passwords, digital certificates, and digital authentication keys.
Encryption:

Encryption ensures that messages cannot be intercepted or read by anyone other than the authorized.
Security management: This is the glue that holds together the other building blocks of a strong security solution.

However, as networks enable more and more applications and are available to more and more users, they become ever more vulnerable to a wider range of security threats. To combat those threats and ensure that e-business transactions are not compromised, security technology must play a major role in today's networks.

Data mining can derive actionable information from large volumes of data. For example, a town planner might use a model that predicts income based on demographics to develop a plan for low-income housing. A car leasing agency might a use model that identifies customer segments to design a promotion targeting high-value customers. To ensure meaningful data mining results, you must understand your data. Data mining algorithms are often sensitive to specific characteristics of the data: outliers (data values that are very different from the typical values in your database), irrelevant Columns, columns that vary together (such as age and date of birth), data coding, and Data that you choose to include or exclude.

Without proper protection, any part of any network can be susceptible to attacks or unauthorized activity. Routers, switches, and hosts can all be violated by professional hackers, company competitors, or even internal employees.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

In fact, according to several studies, more than half of all network attacks are waged
internally. The Computer Security Institute (CSI) in San Francisco estimates that between 60 and 80 percent of network misuse comes from inside the enterprises where the misuse has taken place. To determine the best ways to protect against attacks, IT managers should understand the many types of attacks that can be
instigated and the damage that these attacks can cause to e-business infrastructures. The most common types of attacks include Denial of Service (DoS), password, and root access attacks. *DoS attacks* are particularly malicious because although they do not provide intruders with access to specific data, they "tie up" IS resources, preventing legitimate users from accessing applications. They are usually achieved by hackers sending large amounts of jumbled or otherwise unmanageable data to machines that are connected to corporate networks or the Internet. Even more malicious are Distributed Denial of Service (DDoS) attacks in which an attacker compromises multiple machines or hosts. According to the 2001 Computer Security Institute (CSI) and FBI "Computer Crime and Security Survey," 38 percent of respondents detected DoS attacks, compared with 11 percent in 2000.

To ensure that their networks remain secure, companies should continuously monitor for attacks and regularly test the state of their security infrastructures. Network vulnerability scanners can proactively identify areas of weakness, and intrusion detection systems can monitor and reactively respond to security events as they occur. Intrusion detection systems and vulnerability scanners provide an additional layer of network security. While firewalls permit or deny traffic based on source, destination, port, or other criteria, they do not actually analyze traffic for attacks or search the network for existing vulnerabilities. In addition, firewalls typically do not address the internal threat presented by "insiders." The Cisco Intrusion Detection System (IDS) is the industry's first real-time, network intrusion detection system that can protect the network perimeter, extranets, and increasingly vulnerable internal networks. The system uses sensors, which are high-speed network appliances, to analyze individual packets to detect suspicious activity. If the data stream in a network exhibits unauthorized activity or a network attack, the sensors can detect the misuse in real time, forward alarms to an administrator, and remove the offender from the network. The Cisco Secure Scanner is an enterprise-class software scanner application that allows an administrator to identify and fix network security holes before hackers find them.

SYSTEM DESIGN

INPUT DESIGN

Input design is the process of converting user-originated inputs to a computer-based format. Input design is one of the most expensive phases of the operation of computerized system and is often the major problem of a system.

In the project, the input design is made in various web forms with various methods. For example, in the user creation form, the empty username and password is not allowed. The username if exists in the database, the input is considered to be invalid and is not accepted. Likewise, during the login process, the username is a must and must be available in the user list in the database. Then only login is allowed. The data from the user, the certificate and the puzzle are the inputs.

OUTPUT DESIGN

Output design generally refers to the results and information that are generated by the system for many end-users; output is the main reason for developing the system and the basis on which they evaluate the usefulness of the application.

In the project, the user verification and the data update are the forms in which the output is available.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

DATABASE DESIGN

The database design is a must for any application developed especially more for the data store projects. Since the chatting method involves storing the message in the table and produced to the sender and receiver, proper handling of the table is a must. In the project, login table is designed to be unique in accepting the username and the length of the username and password should be greater than zero. The different users view the data in different format according to the privileges given.

PROPOSED SYSTEM

The proposed system introduces first secure and distributed data discovery and dissemination protocol named DiDrip. It allows the network owners to authorize multiple network users with different privileges to simultaneously and directly disseminate data items to the sensor nodes.

The distributed data discovery and dissemination is an increasingly relevant matter in WSNs, especially in the emergent context of shared sensor networks, where sensing/communication infrastructures from multiple owners will be shared by applications from multiple users. For example, large scale sensor networks are built in recent projects such as Geoss, NOPP and ORION. These networks are owned by multiple owners and used by various authorized third-party users. Moreover, it is expected that network owners and different users may have different privileges of dissemination. In this context, distributed operation by networks owners and users with different privileges will be a crucial issue, for which efficient solutions are still missing. Motivated by the above observations, this paper has the following main contributions:

1) The need of distributed data discovery and dissemination protocols is not completely new, but previous work did not address this need. We study the functional requirements of such protocols, and set their design objectives. Also, we identify the security vulnerabilities in previously proposed protocols.

2) Based on the design objectives, we propose DiDrip. It is the first distributed data discovery and dissemination protocol, which allows network owners and authorized users to disseminate data items into WSNs without relying on the base station. Moreover, our extensive analysis demonstrates that DiDrip satisfies the security requirements of the protocols of its kind. In particular, we apply the provable security technique to formally prove the authenticity and integrity of the disseminated data items in DiDrip.

3) We demonstrate the efficiency of DiDrip in practice by implementing it in an experimental WSN with resource-limited sensor nodes. This is also the first implementation of a secure and distributed data discovery and dissemination protocol.

The proposed DiDrip protocol consists of four phases, system initialization, user joining, and packet preprocessing 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 preprocessing 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. In addition the puzzle game approach has proposed to secure the data transmission path by generating a puzzle from the user to the cluster head. The cluster heads can solves the puzzle when the nods are authorized.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

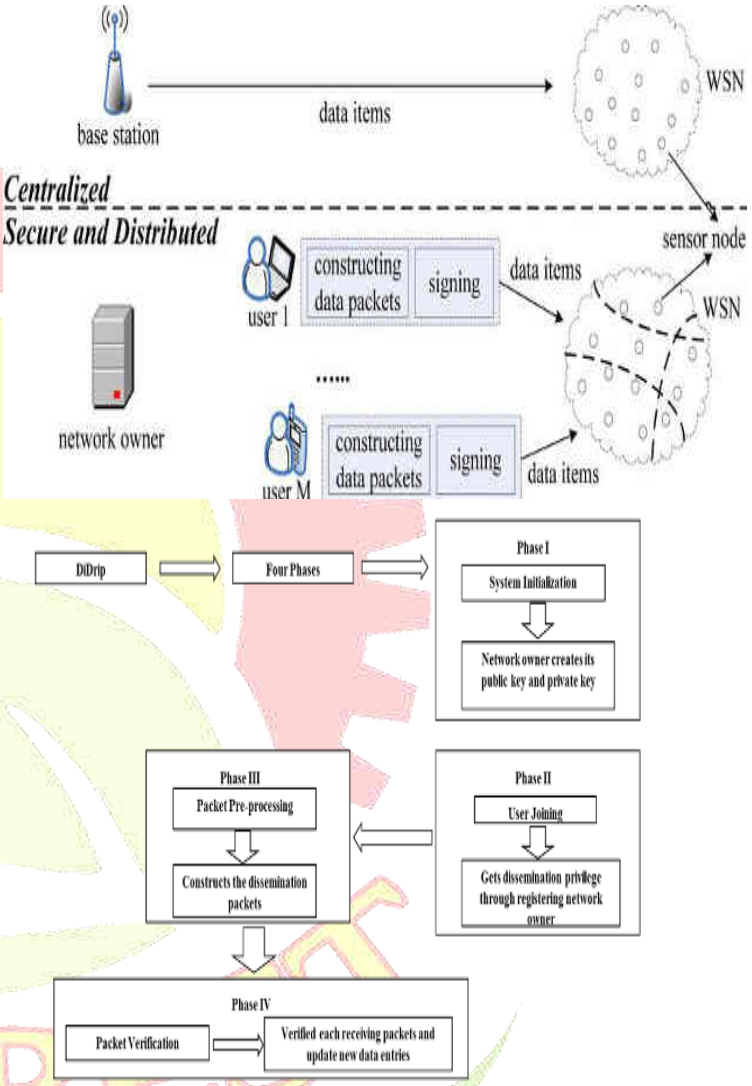
Vol. 2, Special Issue 10, March 2016

To improve the data confidentiality we propose Puzzling approach in wireless sensor nodes. It reduces the dissemination delay, which is the time for a disseminated packet to reach nodes in a WSN.

The node must answer the puzzle within a particular time. So the node which gives the correct puzzle solution

- User can send the data directly to the sensor nodes without using the base station Provide more security for data
- Increase packet delivery ratio.
- These networks are owned by multiple owners and used by various authorized third party users
- Emergent context of shared sensor networks
- It is expected that network owners and different users may have different privileges of dissemination
- It improves data confidentiality by using puzzle based route reconfiguration.

SYSTEM ARCHITECTURE



CONCLUSION AND FUTURE WORK

We have identified the security vulnerabilities in data discovery and dissemination when used in WSNs, which have not been addressed in previous research. Also, none of those approaches support distributed operation. Therefore, we proposed, a secure and distributed data discovery and dissemination protocol named DiDrip. Besides analyzing the security of DiDrip, our approach 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. 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.

A data discovery and dissemination protocol for wireless sensor networks (WSNs) is responsible for updating configuration parameters of, and distributing management commands to, the sensor nodes. All existing data discovery and dissemination protocols suffer from two drawbacks. First, they are based on the centralized approach; only the base station can distribute data items. Such an approach is not suitable for emergent multi-owner-multi-user WSNs. Second, those protocols were not designed with security in mind and hence adversaries can easily launch attacks to harm the network. This paper proposes the first secure and distributed data discovery and dissemination protocol named DiDrip. It allows the network owners to authorize multiple network users with different privileges to simultaneously and directly disseminate data items to the sensor nodes. Moreover, as demonstrated by our theoretical analysis, it addresses a number of possible security vulnerabilities that we have identified. Extensive security analysis show DiDrip is provably secure. To improve the data confidentiality we propose Puzzling approach in wireless sensor nodes. It identifies misbehaving intermediate nodes or cluster heads and eliminates from the data transmission path.

REFERENCES

[1] J. W. Hui and D. Culler, "The dynamic behavior of a data dissemination protocol for network programming at scale," in Proc. 2nd Int. Conf. Embedded Netw. Sensor Syst., 2004, pp. 81–94.

[2] D. He, C. Chen, S. Chan, and J. Bu, "DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1946–1956, May 2012.

[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] M. Ceriotti, G. P. Picco, A. L. Murphy, S. Guna, M. Corra, M. Pozzi, D. Zonta, and P. Zanon, "Monitoring heritage buildings with wireless sensor networks: The Torre Aquila deployment," in Proc. IEEE Int. Conf. Inf. Process. Sensor Netw., 2009, pp. 277–288.

[7] D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks," IEEE Trans. Wireless Commun., vol. 12, no. 9, pp. 46384646, Sep. 2013.

[8] M. Rahman, N. Nasser, and T. Taleb, "Pairing-based secure timing synchronization for heterogeneous sensor networks," in Proc. IEEE Global Telecommun. Conf., 2008, pp. 1–5.

[9] Geoss. [Online]. Available: http://www.epa.gov/geoss/

[10] NOPP. [Online]. Available: http://www.nopp.org/