International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 7
July 2017

Academic Science

Security Analysis of Di-Drip Protocol For Wireless Sensor Network

Anagha Chaphadkar[1] and Dr. Achala Deshmukh[2]
[1]PG student, Digital Systems (Electronics), SCOE, Pune, India
[2]Professor, E&TC, SCOE, Pune, India

ABSTRACT
A responsibility of data discovery and dissemination protocol for wireless sensor networks is updating configuration parameters and distributing management commands to the sensor nodes. The existing system has two drawbacks. First they are based on the centralized approach in which only base station distributes data items. So this type of approach is a single user approach and is not suitable for multi-owner-multi-user wireless sensor networks. Second while designing these protocols they are considering security issues in mind and hence attackers can easily harm network. This protocol named as Di-Drip is secure and distributed data discovery and dissemination protocol. The proposed system allows network owners to authorize multiple network users with different privilege level to simultaneously and directly disseminate data items to the sensor nodes. Moreover, it addresses a number of possible security vulnerabilities that have been identified. Extensive security analysis show Di-Drip is provably secure.

KEYWORDS
Distributed data discovery and dissemination, Wireless Sensor Networks, Efficiency, Network Coding, Security.

1. INTRODUCTION

In centralized approach, data can only be broadcasted by the base station as shown in the top sub-figure in Fig.1. This approach suffers from the single point of failure because when the base station is not functioning properly or when the connection between the base station and a node is broken at that time the transmission is impossible. Even worse, some WSNs do not have any base station at all. For example, for a WSN located in a remote area to monitor illegal crop cultivation, a base station becomes an attractive target. For such networks, data transmission to be carried out by authorized network users in a distributed manner is better.

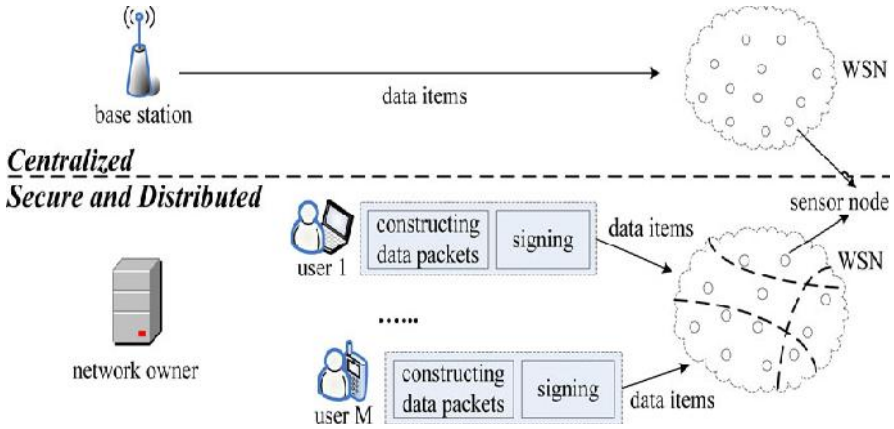

Fig. 1: System overview of centralized and distributed approach. [1]

The number of nodes implementing trickle are required to forward all new data items that they receive. An enemy can introduce denial of service (DoS) attack to the sensor nodes by injecting a large amount of bogus data items. This results into expanded energy resource of nodes for process and forward these bogus data

items. Any data discovery and dissemination protocol based on Trickle or its variants is unprotected from such a DoS attack.

2. LITERATURE SURVEY

Trickle was a code propagation mechanism, but it could be used to broadcast any data. A reliable distribution protocol for broadcasting a large data from multiple source nodes to many other nodes over a multihop wireless network was described in [3].

Deluge was presented in [4], a reliable data dissemination protocol for transmitting a large data object from multiple nodes to many other nodes over wireless sensor network. A simple model of Deluge's can be used to identify different factors which limit the overall bandwidth of any multihop communication protocol.

The DIP was proposed in [2] for wireless networks that scale linearly with the number of data items. DIP follows Trickle's approach of using local wireless broadcasts. For T items, DIP can identify new items with O (log (T)) packets while maintaining an O (1) detection latency.

DHV can be proposed and evaluated in [5], an efficient code consistency maintenance protocol. In DHV, it is not necessary to transmit and compare the whole version in the network. DHV aims to detect and identify differences of version-levels for code items with the goal of transmitting much less data in the network compared with other protocols.

A secure, lightweight, and DoS resistant data discovery and dissemination protocol named SeDrip was developed for WSNs, which is a secure extension of Drip [6]. This protocol considers the limited resources of sensor nodes. It can provide instantaneous authentication and without packet buffering delay and tolerate node compromise.

Di-Code was proposed in [8]. The notable element of Di-Code protocol is capacity to oppose adversary attacks. Theoretical analysis demonstrates about security properties of Di-code.

3. IMPLEMENTATION DETAILS

3.1. System Overview

DiDrip protocol is designed such that network owners and authorized users allowed to transmit data items into WSNs without involving the base station. In particular, the provable security technique can be applied to prove the authenticity and integrity of the disseminated data items.

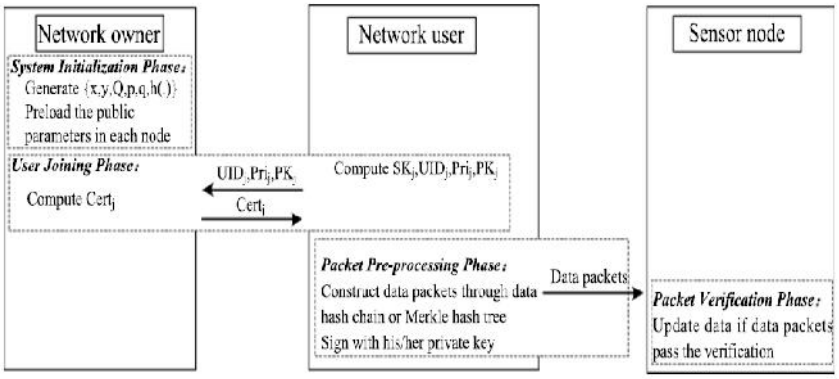

Fig. 2: System phases. [1]

While implementing this protocol, the security vulnerabilities in previously proposed protocols can be identified. DiDrip protocol consists of four phases, system initialization, user joining, packet pre-processing and packet verification. The information processing flow of DiDrip is illustrated in Fig.2. DiDrip protocol uses a digital signature to computing the authentication of data discovery and dissemination. This authentication is unprotected from DoS attacks. Hence the message specific puzzle is introduced to reduce the

dissemination delay, which is the time for a disseminated packet to reach all nodes in a WSN. There are two characteristics of the puzzles. First, the puzzles are difficult to be solved but their solutions are easy to be verified. Second, there is a tight time limit to solve a puzzle. This discourages an enemy to introduce the DoS attack even if they are computationally powerful.

3.2. Mathematical Model

System Initialization Phase:

Elliptic curve cryptography is used for the encryption and decryption of messages. 160 bit ECC is set up in this phase. Choose two big prime numbers p and q which is 160 bit long.

1. Select an elliptic curve E over GF(p)
2. Select private key x ϵ GF(q).
3. Compute the public key y = x*Q where Q is the base point of E.
4. Load the public parameters {y, Q, p, q} in each node.

User Joining Phase :

When any user, say Uj wants to join the network and gets the transmission privileges, the user joining phase is invoked. The user requests for the certificate from the network owner. Consider Uj is user with the identity UIDj. Chooses a private key SKj ϵ GF(q)

1. User computes the public key PKj = SKj.Q
2. User sends a 3-tuple < UIDj, Prij, PKj> to the network owner.
3. The network owner generates the certificate and sends back to the user Uj.
4. Certj= {UIDj,PKjPrij, SIGx{h(UIDj || PK || Prij)}}

Packet Pre-processing Phase:

After user enters into the network packet pre-processing phase will start. User has some information to transmit over the network, first it has to construct the data packet.

1. The user constructs the packet by using Merkle hash tree method.
2. Here a tree is constructed taking n data items.
3. The data items act as the leaves of the tree.
4. At the upper level, internal nodes are constructed by concatenating two child nodes.
5. Continue constructing the nodes until the root node is formed. It is labelled as Hroot.
6. Thus obtained tree is the Merkle hash tree with depth D = logn(n).
7. The user, before dissemination of actual data items, Signs the root node Hrootwith SKj.
8. Sends an advertisement packet P0.

The user sends further packets when P0 = {Certj || Hroot|| SKj(Hroot)}, has been sent. In Merkle hash tree method, each packet contains the D hash values.

Packet Verification Phase:

When any sensor node receives the transmitted data, it has to first verify whether it is from authorized user, whether that sensor node ID is included in the node identity set of Prij and whether the packet maintains data integrity.

1. If the packet received is advertisement packet
2. Check for the privileges.
3. If the result is positive, then check for the authenticity
4. If certificate is valid, check for the validity of signature.
5. If the result is positive then store <UIDj, root>, otherwise discard the packet.
6. If the packet received is a data packet other than P0, the sensor node checks for the authenticity and integrity.

3.3. System Specification

Functional Requirements:

1. Distributed: Multiple authorized users should simultaneously transmit data items into the WSN without involving the base station.

Academic Science

2. Supporting different user privileges: Network owner should provide certain privilege level to each user for flexibility.
3. Authenticity and integrity of data items: Only data transmitted by authorized users should be accepted by a sensor node.
4. User accountability: Users must have some accountability for joining the network to avoid bad user behaviors and insider attacks.
5. DoS attacks resistance: The functions of the WSN should not be damaged by DoS attacks.
6. Freshness: A node should be able to differentiate whether an incoming data item is the newest version.

Non-functional Requirement:

1. Performance Requirements: If any of the mentioned requirements is absent in the system then performance will be affected. Hence system should be well designed to maintain its performance and to resist the system from black hole attacks.

2. Security Requirement: Unauthorized users should be prohibited from accessing the system. Password authentication and accounting of every authorized user should be introduced to prevent insider attacks as well as other adversary attacks.

2.4. Implementation status

User accountability can be satisfied by introducing login page into the network for preventing the system from all type of attacks. All the users can get some transmission privileges after completion of user joining phase. This provides a unique username and password to every user who wishes to join the network. The DiDrip is implemented by designing graphical user interface (GUI). The GUI consists of number of keys such as total number of nodes, source node, destination node, attacker node, change of path, etc. In the simulation, GUI is used for the network creation. After entering all the fields in GUI, user need to click on draw node button.

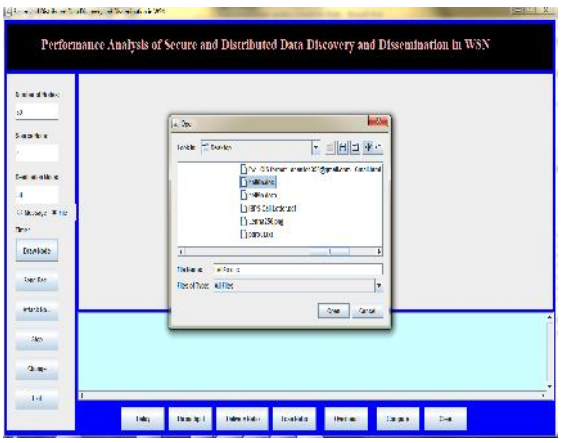

Fig. 3: Simulated result for DiDrip algorithm in WSN with file Selection window.

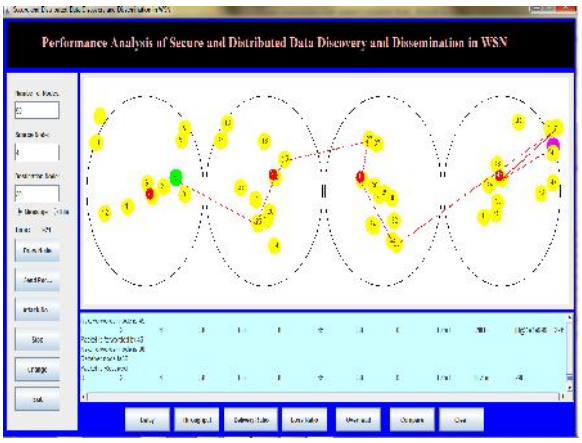

Fig. 4: Simulated result for DiDrip algorithm in WSN with display of shortest distance path.

There are three types of data can be disseminated using this protocol such as image, message and documents including text, doc and docx files. So user has to choose the option according to type of data which user wants to disseminate. For example if user wants to send image or document file then he/she needs to choose file option and select file from the “File Selection” window as shown in Fig. 3. After typing a message or selecting a file and clicking on “OK” button, the network simulator creates WSN by using graphical view and displays the shortest distance path for data dissemination. The network creation is presented in Fig 4. RSA algorithm is used for the encryption and decryption of the message which is an asymmetric cryptographic algorithm. Confidential data transfer such as images and documents are demonstrated by AES algorithm which is a symmetric encryption algorithm. Image dissemination is shown in Fig. 5.

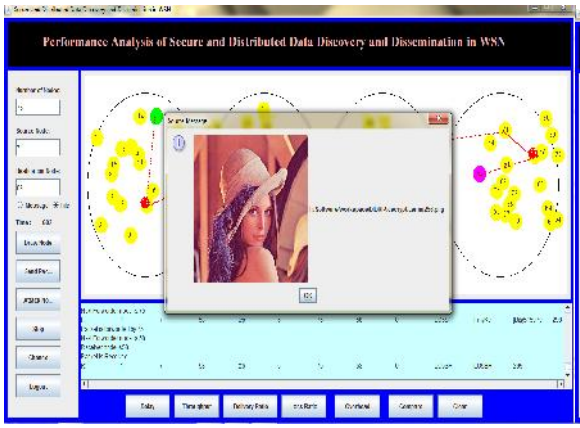

Fig. 5: Simulated results for dissemination of image data.

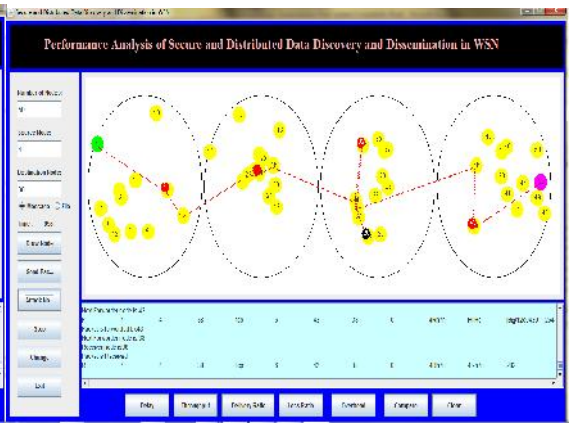

Fig. 6: Simulated results for changing path after detection of black hole attack.

To prevent black hole attacks multipath routing algorithm is used. This algorithm has many advantages such as fault tolerance, increased bandwidth and improved security. If any black hole attacker node is detected along the path, then it automatically switch to the another path. Hence multiple alternative paths are selected in this technique by using shortest distance path method. For shortest distance path selection, Euclidean distance algorithm is utilized. The changing of path after detection of black hole attack is shown in Fig. 6.

Performance Analysis:

The system analyses the performance by using performance parameters such as delay, throughput, packet delivery ratio, packet loss ratio, overhead, etc. System also compares performance before and after black hole attack detection. Additionally system compares its simulation results with Drip so as to analyse the performance of the system and validation of results. Fig.7a shows packet transmission delay ratio. This delay is reduced due to energy efficient packet data transmission using shourtest path selection routing. Fig.7a also shows that how delay is initially high in existing system Drip but it is decressed in DiDrip. It is defined as the total number of packets delivered over the simulation time. Fig.7b shows throughput for packet transmission. The throughput is increased in DiDrip compared with Drip. In the proposed system security is provided by using AES algorithms. Also attack detection and prevention is done with the use of multipath routing algorithm. Hence packet loss ratio is increased. PDR is presented in Fig.7c. DiDrip reduces packet loss ratio in WSN with energy efficient packet transmission by avoiding attacker nodes. The Packet Loss ratio is shown in Fig.7d. The DiDrip protocol is implemented to avoid Attacks in wireless sensor network. Various encryption algorithms are used to avoid overhead for authentication each time. Hence the overhead is minimized in the proposed system as compared with the existing system. Fig.7e shows overhead ratio. In the comparison, analysis of PDR and PLR with and without attacker is shown. The effect on the performance before and after detection of black hole attack is analysed and minimized by using multipath routing algorithm. It is presented in Fig.7. All the performance parameters demonstrated in DiDrip provides better result than existing system. This can be analysed by Fig.7. which is shown below.

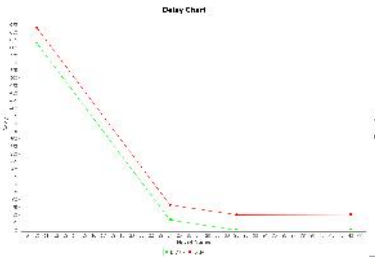

Fig. 7a: Delay

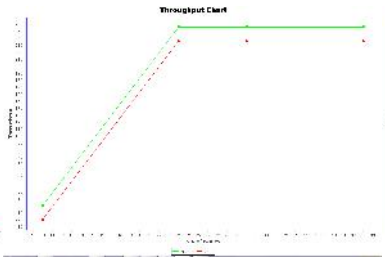

Fig. 7b: Throughput

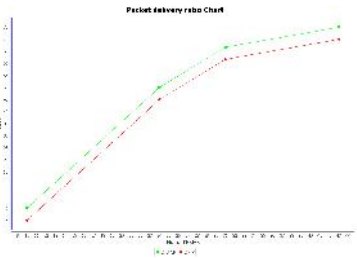

Fig. 7c: Packet Delivery Ratio

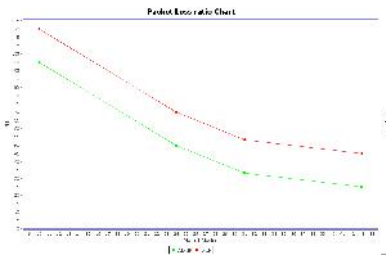

Fig. 7d: Packet Loss Ratio

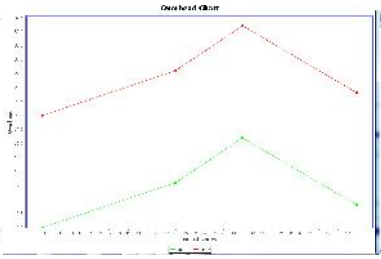

Fig. 7e: Overhead

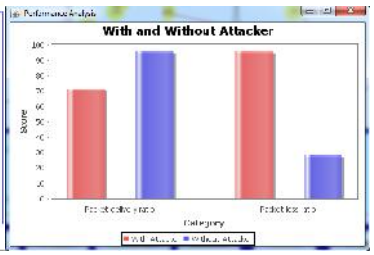

Fig. 7f: Comparison

Fig. 7: Performance Parameters.

Security analysis is the main featude discussed and implemented in proposed system. Hence all parameters are implemented on basis of security analysis and attack prevention.

4. CONCLUSIONS

DiDrip protocol achieves secure and fast data dissemination. This technique combines the concepts of network coding and simple cryptographic techniques for transmission of data. This protocol provides a better security against pollution attacks, and achieves immediate authentication of data been disseminated. Performance analysis is done by using various parameters such as delay, throughput, overhead, packet delivery ratio and packet loss ratio. Comparison chart is also demonstrated for before and after detection of black hole attack. The secure transfer of confidential data like text, images is also demonstrated using advanced algorithms. Hence it aims to provide a simple yet secure and fast data dissemination for wireless sensor networks. Node compromise by an attacker can be an issue in this protocol. It will be the part of the future works.

REFERENCES

[1] D. He, S. Chan, H. Yang And B. Zhou, "Secure And Distributed Data Discovery And Dissemination In WSN", IEEE Transactions On Parallel & Distributed S/m, Vol. 26, No. 4, April 2015

[2] 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.

[3] 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. 4638–4646, Sep. 2013.

[4] 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.

[5] G. Tolle and D. Culler, "Design of an application-cooperative management system for wireless sensor networks," in Proc. Eur. Conf. Wireless Sensor Netw., 2005.

[6] 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.

[7] P. Levis, N. Patel, D. Culler, and S. Shenker, "Trickle: A self-regulatingalgorithm for code maintenance and propagation in wireless sensor networks," in Proc. 1st Conf. Symp. Netw. Syst. Design Implementation, 2004, pp. 15–28.

[8] A. Perrig, R. Canetti, D. Song, and J. Tygar, "Efficient and secure source authentication for multicast," in Proc. Netw. Distrib. Syst. Security Symp., 2001.

[9] Lekhana D N "A Novel Approach for Secure and Distributed Data in Cluster Based Wireless Sensor Network" (Volume-5, Issue-5) in Proc. IEEE Security Privacy, 2016.

[10] "Distributed and Secure DiDrip Protocol for Data Discovery and Dissemination in WSNs", International Journal of Innovative Research in Science, Engineering and Technology (Vol. 5, Issue 4, April 2016)