INTEGRATION OF SECURITY AND AUTHENTICATION AGENT IN NS-2 AND LEACH PROTOCOL FOR WIRELESS SENSOR NETWORK

Tin Win Maw

Department of Information and Communication Technology, University of Technology (Yantanarpon Cyber City), Pyin-Oo-Lwin City, Myanmar

ABSTRACT

Wireless Sensor Networks (WSN) is an emerging technology for attraction of researchers with its research challenges and various application domains. Today, WSN applications can be used in environmental detection, Monitoring system, medical system, military and industrial monitoring for ability to transform human life in various aspects. Depending on applications used for WSNs, security is the biggest challenges in WSNs and security aspect is essential for WSNs before designing WSNs. The routing protocols for WSNs need security services for transmission exact and secure data to the users through the network. LEACH (Low Energy Adaptive Clustering Hierarchy) is a routing protocol used in WSNs by arranging sensor nodes into clusters. Every sensor cluster is managed by a Cluster Head (CH) during the network operation such as routing and data aggregation from Cluster Member (CM). Therefore, security and authentication is necessary between CH and CM. However, LEACH is lack of security. This paper presents integration of security and authentication between CH and CM on LEACH routing protocol. For the implementation of this integration, NS-2 simulation software is used and it is necessary to combine security agent into NS-2 tool for WSN. But currently, NS-2 does not support these features. Therefore, the main aim of this paper is to develop security and authentication agent into NS-2 and LEACH protocol for WSNs with the simulation results.

KEYWORDS

Wireless Sensor Network, NS-2, Authentication, Security, LEACH

1. INTRODUCTION

WSNs have become most interesting research area because of its useful inherent characteristics such as power, small volume, scalability of nodes, easy to use etc. Day by day, many usages of WSN applications in hostile environments are being needed for demand of today's world because of many natural disasters like earthquakes, flooding, Tsunamis and forest firing, etc. Currently, WSNs have provided usefulness to several important field areas such as environmental monitoring like flood and forest firing detection, industrial monitoring like status monitoring, medical like Body Sensor Network (BSN), military like reconnaissance of opposing forces and other monitoring systems like air, water and animals . Depending on applications used for WSNs, security is the biggest challenges in WSNs and security aspect is essential for WSNs before designing WSNs. The resource constraints and limitations make WSNs most challenging research area such as energy and vulnerable to lack security.

DOI : 10.5121/ijitmc.2014.2206

There are many WSN routing protocols for data transmission to the used from the network. The hierarchical routing protocols are used for optimizing energy consumption for sensor nodes by arranging sensor nodes into clusters. Every sensor cluster is managed by a CH during the network operation such as data transmission. LEACH (Low Energy Adaptive Clustering Hierarchy) is a hierarchical routing protocol used in WSNs. But LEACH routing protocol is lack of security. LEACH arranges the nodes in the network into small clusters and chooses one of them as CH. Non CH nodes (CM) senses in a specific area and then sends the relevant information to its CH. Then the CH aggregates the information received from all the nodes and sends it to the base station. LEACH elects CH from all nodes randomly. There is necessary to have authentication between CH and CM to ensure that the exact CMs send data to CH within a cluster. If only a CM compromises, the whole network will be compromised. This paper presents integration of authentication between CH and CM on LEACH routing protocol by using NS-2 simulation tool. The Figure 1 shows LEACH protocol.

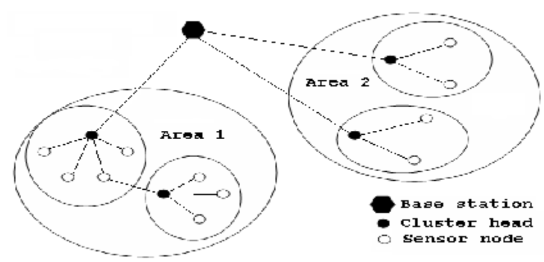

Figure 1. LEACH protocol data transmission

NS2 is one of the most network simulation tools and it is an open source tool that is developed using C++ and Object Tool command Language (OTCL). Researcher can freely add new components and routing agents to the system to serve their own purpose. In order to integrate security and authentication agent for network, it is needed to add security functions into NS-2. For the purpose of analysis, this paper uses the key is pre-shared key system and the encryption/and decryption algorithm is RC4 stream Cipher and CESAR cipher. Because of complexity of other hash algorithms, the hashing algorithm to provide authentication is very simple polynomial algorithm [1].

2. CHARACTERISTICS AND CHALLENGES OF WSN

Currently, WSNs have provided usefulness to several important field areas such as because of the useful characteristics such as

- Power consumption constraints for nodes using batteries
- Ability to cope node failures
- Mobility of nodes
- Dynamic network topology
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental condition
- Ease of use etc.

Because of these useful characteristics, they have limitations and constrainsts. In WSN, sensor nodes have

- Tiny device, small in volume
- Limited storage capacity
- Limited resources
- Limited processing power consumption and radio ranges
- Communication bandwidth
- Storage space
- (Battery based)

This gives rise to new and unique challenges in data management and information processing such as energy and security. Therefore, in order to develop useful resources efficient mechanisms for WSN, it is necessary to know and understand these constraints first in [2] and [3]. The energy and security are biggest challenges in WSN.

2.1. Security challenges in WSN

Designing security is a challenging task for a WSN because of following characteristics [4]

- Wireless channels are open to everyone thus any can monitor in communication in a wireless channel.
- Most protocols for WSN did not consider necessary security mechanism.
- Different to implement stronger security mechanism on sensor platform due to their complexity.
- Strong protocol costs more resources in sensor nodes which can lead to performance degradation of applications.
- Deployed in hostile environment without any fixed infrastructure. Therefore it may face various attacks.

2.2. Security requirements of WSN

It is necessary to know and understand these security requirements first before implementing security scheme for WSN.WSN should take the following major security requirements which are basic requirements for any network into consideration of secure mechanism.

2.2.1. Data Integrity

Data integrity in sensor networks is needed to ensure the reliability of the data [5]. It ensures that data packets received by destination (CH) is exactly the same with transferred by the sender (CM) and any one in the middle cannot alter that packet. Data integrity is achieved by means of authentication the data content [2].

2.2.2. Data Authentication

Data Authentication of a sensor node ensures the receiver that the data has not been modified during the transmission [6]. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys.

2.2.3. Data Confidentiality

Data confidentiality of the network means that data transfer between sender and receiver will be totally secure and no third person can access it (neither read nor write) [3]. Confidentiality can be achieved by using cryptography: symmetric or asymmetric key can be used to protect the data [2].

2.2.4. Data Availability

Data Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. It should be ensured that security mechanisms imposed for data confidentiality and authentication are allowing the authorized nodes to participate in the processing of data or communication when their services are needed [6].

2.3. Security Attacks in WSN

Any actions that compromises the security of information owned by an organization or person is called security attack. These attacks classified into two main categories [7].

1. Passive attacks
2. Active attacks.

2.3.1. Passive Attacks

Passive attacks are the attacks in which an attacker does not actively participate in bringing the network down. A passive attacker attempts to learn or make use of information from the network. The attacker can then forward this information to an accomplice who in turn can use it to launch attacks to bring down the network.

2.3.2. Active Attacks

Active attacks are the attacks in which an attacker actively participates in disrupting the normal operation of the network services. The attacker drops packets, modifies packets, fabricates messages or pretends to be as some other nodes; nodes rush packets or tunnel them over high-speed private networks to an accomplice in other part of the network, etc.

2.4. Denial of Service Attacks in WSN

Denials of Service attacks are specific attacks that attempt to prevent legitimate users from accessing networks, servers, services or other resources. While DOS attacks continues to evolve, the circumstances that enabling attacks have not significantly changed in recent year. There are various kinds of DOS attacks which can cause in and decrease network life time in different ways. The followings are some of DOS attacks.

- Jamming attack
- Sybil attack
- Sinkhole/Black hole attack
- Wormhole attack
- Flooding attack
- Selective forwarding attack
- Spoofing attack
- Replay attacks

This paper develops integration of the security into NS-2 and LEACH in WSNs to provide authentication between CH and CM during data transmission.

3. LOW ENERGY ADAPTIVE CLUSTERING HIERARCHY (LEACH) PROTOCOL IN WSN

LEACH is a cluster-based and energy conserving routing protocol. LEACH operations can be divided into two phases. LEACH operation is broken into rounds, with each round having a set-up phase and a steady state phase [10].

In the setup phase, the clusters are formed and a CH is chosen for each cluster from among all nodes. During the steady phase, data is sensed and sent to the BS. LEACH elects CH from all nodes randomly. LEACH organizes nodes into clusters with one node from each cluster serving as a CH. It randomly selects some predetermined number of nodes as cluster heads. CHs then advertise themselves and other nodes join one of those cluster heads [10]. In this way a cluster is formed.

The CH then makes a Time Division Multiple Access (TDMA) schedule for the nodes under its cluster. The communication between different clusters is done through CHs in a Code Division Multiple Access (CDMA) manner. The CHs collect the data from their clusters and aggregate it before sending it to the other CHs or base station (BS).

After a predetermined time lapse, the cluster formation step is repeated so that different nodes are given a chance to become CHs.

4. SIMULATING OF INTEGRATION FOR SECURITY AGENT IN NS-2 AND AUTHENTICATION IN LEACH

In order to integrate security and integrity features into NS-2 and LEACH for wireless sensor network, we need to add security and authentication Agent into NS-2. The purpose of this paper is only to illustrate a way to add security and authentication Agent into NS-2 and LEACH for wireless sensor network.

Our approach is to build a new Agent at network layer. We also define new packet format to represent new protocols. The new protocol is represented by a class derived from built-in class in NS-2 (**Agent/Authen_Agent**). Within new derived class we will implement hash generation function to ensure the authentication of data packet during transmission. We will also add encryption and decryption for the modified data packet. For development of this integration of security and authentication Agent in to NS-2 tool developer need following environment development requirements:

- Personal Computer Laptop with Open SUSE Linux 11.3
- NS- 2.34 or NS-2.35 version
- LEACH protocol integration
- C/C++ editor
- Programming skill: C++ and TCL

The implementation process to integrate new authentication Agent to NS-2 is shows in [8] [9]. The new packet class is created in a folder under NS-2 directory, for example (**mkdir ns-2.34/Authen**). After that, the new packet name has to register to the packet.h under (**ns-**

2.34/common). Of course, the makefile (**ns-2.34/Makefile**) has to be modified by inserting new Agent class so that the new class is complied.

At the TCL layer, the new packet must be declared by adding the name and default packet size value to the ns-default.tcl (**ns-2.34/tcl/lib/ns-default.tcl**) file.

Finally, we have to make an entry for the new packet in the ns-packet.tcl (**ns-2.34/tcl/lib/ns-packet.tcl**) file.

After recompile the ns-2 with command (**make clean and make**), we can use the new packet for our simulation [8].

The Figure 2 shows the procedure how to integrate a new Agent into NS-2. This paper implements a new agent carrying data. The methods of new class include RC4 and CESAR encryption and decryption as well as generate hash function for authentication. This shows in Figure 3. The hash generator is polynomial hash function in C++ for authentication.

In RC4, the message is encrypted bit by bit with a pre-shared symmetric key by sender and is decrypted with the same key by the receiver.

In CESAR, The key is an integer from 1 to 25. This cipher rotates the letters of the alphabet (A to Z). The encoding replaces each letter with the 1st to 25th next letter in the alphabet (wrapping Z to A). The polynomial hash function is shown in Figure 4.

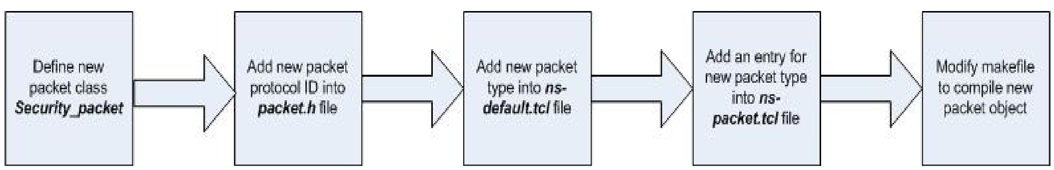

Figure 2. Procedure to integrate new authentication Agent to NS-2 and LEACH

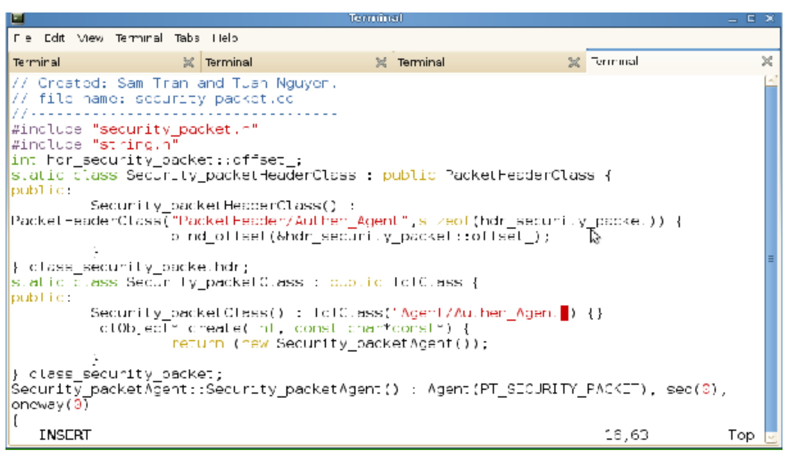

Figure 3. New authentication Agent class

```
unsigned int Security packetAgent::hashing(char value[], unsigned int len)
{
  char *word = value;
  unsigned int ret = 0;
  unsigned int i;
  for(i=0; i < len; i++)
  {
    int mod = i % 32;
    ret ^=(unsigned int) (word[i]) << mod;
    ret ^=(unsigned int) (word[i]) >> (32 - mod);
  }
  return ret;
}
```

Figure 4. Polynomial Hash Function

5. SIMULATING OF INTEGRATION FOR AUTHENTICATION IN LEACH

In this simulation experiments, we use NS-2 (version 2.34), a discrete event simulator widely used in the networking research community to investigate how various routing protocols perform with different network configurations. Simulation setup parameters for testing of integration authentication in LEACH are shown in Table 1. The numbers of nodes are from 20 up to 100 with simulation time 100 seconds. The Figure 5 is Nam Animation output of NS-2 for sensor node creation on LEACH protocol. For integration authentication in LEACH, the simulation uses new security Agent (Authen_Agent) class and RC4 and CESAR algorithms as shown in Figure 6, 7 and 8.

In order to test for authentication between CH and CM sensor nodes over LEACH in WSN, the Tcl simulation script is shown in figure 9. Before deploying in the network, the sensor nodes must register with base station with pre-shared key system. Then CH election is performed and forming cluster as LEACH protocol. When CM transmits data to its CH, the authentication Agent is added to provide authentication between CH and CM. This paper simulated this with both RC4 and CESAR encryption and decryption algorithm and polynomial hash fumction. The hash value will be attached to packet header for authentication checking. At the end of communication, after decryption, the decrypted text will be hash again to get new hash value to compare original hash. If they are equal, the data is ensured authentication between nodes, otherwise, the data is discard.

Table 1. Simulation Parameters

	Parameters	Values
1	Simulation area	1000m x 1000m
2	Channel Type	Phy/Wireless channel
3	Radio Propagation Model	Two way ground
4	Max. numbers of nodes	20 up to 100
5	Simulation time	100sec
6	Mac Protocol	Mac/Sensor
7	Energy Model	Battery
8	Interface Queue Type	Queye/DropTail/Priqueue
9	Link Layer Type	LL
10	Communication model	Bi-direction
11	Minimum packet	30
12	Antennae model	Antenna/Omniantenna
13	Initial Energy	2 Joules
14	Agent	Authen_Agent

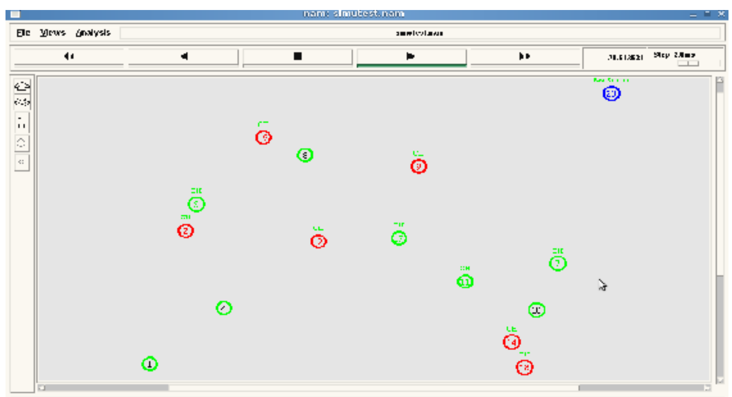

Figure 5. Sensor Node Creation over LEACH for WSN

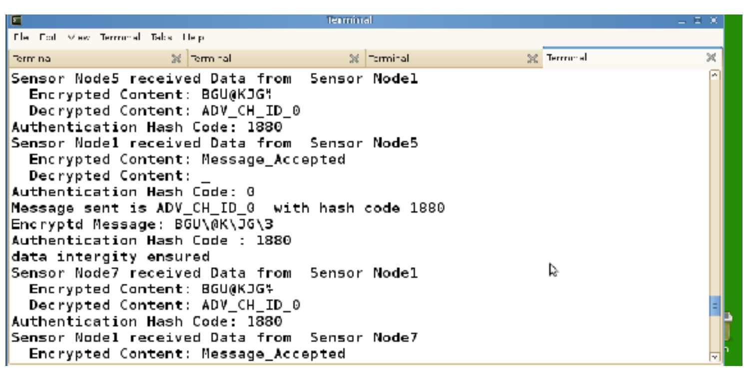

Figure 6. Integration of authentication using RC4

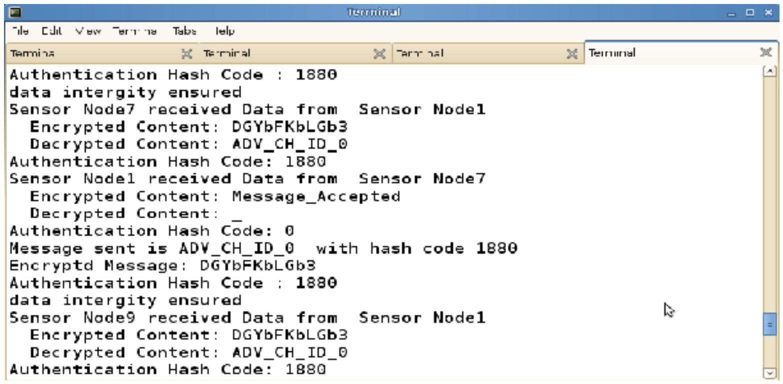

Figure 7. Integration of authentication using CESAR

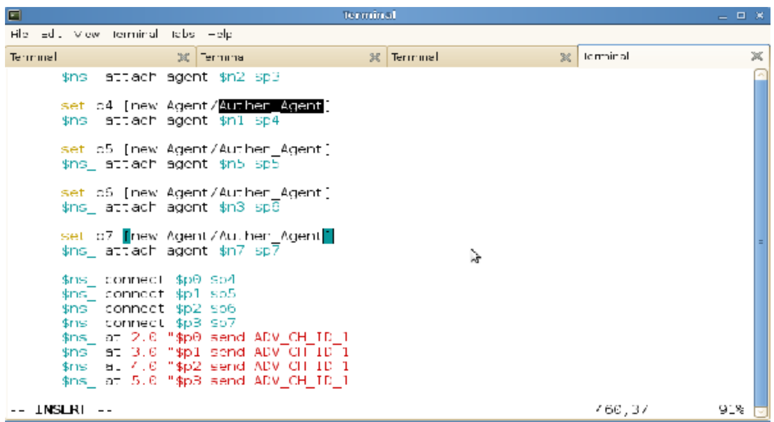

Figure 8. Tcl simulation script to test authentication in LEACH in WSN

6. CONCLUSIONS

This paper simulates an integration of new security authentication Agent into NS-2 and LEACH routing protocol for WSN by using existing one feasible instance encryption/decryption (RC4 and CESAR) and hash algorithm. As further analysis, more security and authentication agent into NS-2 using hashing algorithms such as SHA-256, SHA-384, SHA- 512, etc and DES, RC5, AES, etc for encryption /decryption. With this approach researchers can also add his or her own combined security and integrity Agent into NS-2 by introducing new encryption/decryption and hash algorithm.

ACKNOWLEDGEMENTS

It is my immense pleasure to express my deep sense of gratitude and indebtedness to my highly respected and esteemed and thanks to my supervisor Mr. Myo Hein Zaw, Associate Professor, Principal of Computer University (Monywar), Myanmar for providing and supporting me many suggestions to do my research work. His invaluable guidance, inspiration, constant encouragement sincere criticism and sympathetic attitude could make this paper possible. I express my thanks to my Institution namely University of Technology (Yantanarpon Cyber City) for providing me with a good environment and facilities like internet books, computers and all that as my source to complete this research.

REFERENCES

[1] Hash function implemented in C++ with polynomial algorithm. Retrieved 4/14/05 from http://wikisource.org/wiki/Polynomial_hash_function.

[2] Ace Dimitrievski, Biljana Stojkoska, Kire Trivodaliev, Danco Davcev (2006), "Securing communication in WSN trough use of cryptography", NATO-ARW, Suceava

[3] Muazzam A. Khan, Ghalib A. Shah, Muhammad Sher (2011), "Challenges for Security in Wireless sensor Networks (WSNs)", World Academy of Science, Engineering and Technology

[4] Shio Kumar Singh, M P Singh, D K Singh (2011), "A Survey on Network Security and Attack Defense Mechanism for WSN", Internal Journal of Computer and Technology

[5] G. Padmavathi, D. Shanmugapriya (2009), "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2.

[6] Prajeet Sharma, Niresh Sharma, Rajdeep Singh (2012), "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network", International Journal of Computer Applications Volume 41– No.21.

[7] Siddhartha Gupte and Mukesh Singhal (2003), "Secure routing in mobile wireless ad hoc networks"

[8] Vijayakumar, P. and C. Manikandan, 2010. "Security Function Integration into NS-2 for WSN", National Conference on Information and Software Engineering

[9] http://Marc Greis' Tutorial for the UCB_LBNL_VINT Network Simulator ns .html.

[10] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan (2000), " Energy-Effcient Communication Protocols for Wireless Microsensor Networks (LEACH)," in HICSS,vol. 8, Maui, Hawai, pp. 3005–3014.

Author

Tin Win Maw is a PhD candidate from University of Technology (Yantanarpon Cyber City) (UTYCC). She has received the Degree of Master of Technology from the University of Computer Studies (UCSY, Yangon). The work of her master thesis is "Performance Analysis of Symmetric Encryption Algorithms". She also studied network course at the Information and Communication Technology Training Institute (ICTTI) which is established by UCSY in coordination with Japan International Cooperation Agency (JICA) and programming for network at India Myanmar Centre for Enhancement of Its Skills (IMCEITS). At present, she is working as a tutor at the faculty of information and technology from the (UTYCC).