Australian Journal of Basic and Applied Sciences, 7(7): 376-382, 2013
ISSN 1991-8178

Combined Security and Integrity Agent Integration into NS-2 for Wired, Wireless and Sensor Networks

[1]C.Manikandan, [2]R.Parameshwaran, [3]K.Hariharan, [4]N.Kalaimani, [5]K.P. Sridhar

[1]Assistant Professor-II, Department of ECE,SASTRA University,Tamilnadu,India.
[2, 3]Assistant Professor-II, Department of ICT,SASTRA University,Tamilnadu,India.
[4, 5]PG scholar, Department of VLSI Design,SASTRA University,Tamilnadu,India.

Abstract: The information transmitted over wired, wireless and sensor network can be easily intercepted by third parties, so security issue becomes a central concern. In this project NS-2 simulation software is used. NS-2 is an open source tool that is developed using C++ and Object Tool command Language (OTCL). Implementation of combined security and integrity agent into NS-2 tool is necessary for wired, wireless and sensor networks simulation. However, currently NS-2 tool does not support these features. The purpose of the project is to develop combined security and integrity agent into NS-2 tool for wired, wireless and sensor networks. Our approach is to develop a new packet class carrying data. The methods of the class include some suitable algorithms for encryption and decryption as well as to generate message digest functions for integrity. We know that the security and integrity algorithm which is developed for wired and wireless network is not feasible wireless sensor network. First we implemented industry standard RSA and SHA-1 to demonstrate security and integrity of data transmission for Wired and Wireless networks. Latter we also implemented a simple CESAR cipher and Polynomial hash algorithm to demonstrate security and integrity of data transmission for resource constraint wireless sensor networks .The output of the project shows the security and integrity of data transmission for wired, wireless and sensor network environment in NS-2.

Key words: Wired; Wireless; Sensor Network; NS-2; Security; Integrity

INTRODUCTION

Already many security and integrity algorithms developed for wired networks, it is important to understand that we have more security challenges in wireless networks than in wired networks. In wireless network communications takes place "through the air" using radio frequencies, the risk of interception is greater than with wired networks (Min-kyu Choi, *et al* 2008). If the message is not encrypted, the attacker can read and modify the content in the packet during transmission. In case of wireless sensor network, the communication among the sensors is similar to that of the wireless network but providing security in wireless sensor networks is even more difficult than in wireless networks due to the resource constraints of sensor nodes (Hao Yang, *et al* 2006). Although wireless and wireless sensor networking alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems.

1.1 Wired vs Wireless Networks:

Wireless networks have offered attractive flexibility to both network operators and users. Ubiquitous network coverage, for both local and wide areas, is provided without the cost of deploying and maintaining the wires. This fact is extremely useful in several situations like prohibition of cable deployment and deployment of a temporary network. Mobility support is another salient feature of wireless networks. Even though security threats against the TCP/IP stack in a wired network are equally applicable to an IP-based wireless network, we have number of additional threats (Hao Yang, *et al* 2006); Passive Eavesdropping and Traffic Analysis, Message Injection and Active Eavesdropping, Message Deletion and Interception, Masquerading and Malicious AP, Session Hijacking, Man-in-the-Middle, Denial of Service.

1.2 Wireless Networks vs WSN:

WSN is used in many interesting applications. In wireless sensor network, the communication among the sensors is similar to that of the wireless network but security and integrity algorithm have been proposed for traditional wired and wireless networks are not well suited to the unique features and application requirements of sensor networks. To illustrate this point, the differences between sensor networks and wireless networks are given below (Yong Wang, *et al* 2006):

1. The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in a wireless network.

Corresponding Author: C. Manikandan, Assistant Professor-II , Department of ECE,SASTRA University,Tamilnadu,India.
E-mail: cmanikandan87@gmail.com

2. Sensor nodes are densely deployed.
3. Sensor nodes are prone to failures.
4. The topology of a sensor network changes very frequently.
5. Sensor nodes mainly use a broadcast communication paradigm, whereas most wireless networks are based on point- to-point communications.
6. Sensor nodes are limited in power, computational capacities, and memory. Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.

1.3 The Organization of This Article:

In this paper first, in the Material and Methods section we will talk about some existing security attacks and security services for wired, wireless and sensor networks. Then in the same section we will establish security and integrity agent integration in to NS-2 tool. Afterwards in result section we will show the secure and integrity of data transmission for wired, wireless and sensor network. Finally, in conclusion section, we will present our conclusions and recommendations for future work

MATERIALS AND METHODS

2.1 Security Attack:

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 (Siddhartha Gupte, *et al* 2003):

1. Passive attacks
2. Active attacks.

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.

Active Attack:

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.

2.2 Security Services:

In short, we can say the goal of security is to provide security services to defend against all the kinds of threat. Security services include the following (Erdal Cayirci, *et al.,* 2009):

Authentication:

This service is to verify a user's identity and to assure the receiver that the message is from the source that it claims to be from. Consider a person, using online banking service. Both the user and the bank should be assured in identities of each other.

Access-control:

This service limits and controls the access of a resource such as a host system prevents unauthorized access to a resource. In online banking a user may be allowed to see his balance, but not allowed to make any transactions for some of his accounts.

Confidentiality:

This service ensures that the data/information transmitted over the network is not making known to unauthorized users. Confidentiality can be achieved by using different encryption techniques such that only legitimate users can analyze and understand the transmission.

Integrity:

This service is to assure that the data received are exactly as sent by an authorized party. That is, the data received contain no modification, insertion and deletion.

Non-repudiation:

This service Provides protection against denial by one of the persons involved in communication .This service provides proof of origin and delivery of information. On the Internet, a digital signature is used provides proof of origin and delivery of information.

2.3 Implementation combined of Security and integrity Agent into NS-2:

NS-2 is an open source system that is developed using C++ and Tool command Language (TCL). Researchers can freely add new Agent into NS-2 for their own research purpose. The latest version of NS-2 is version 2.35. Within this version, most of the standard protocols supported. You can find protocol from media access layer protocols such as ALOHA, Slotted ALOHA, CSMA, CSMA/CD and CSMA/CA to application layer protocols as CBR, FTP, TELNET and HTTP. For routing protocols, there are unicast and multicast routing protocols for wire network and DSR, DSDV, AODV, AOMDV, OLSR and ZRP for wireless networks. Most of these protocols were developed by researchers and adopted into standard version of NS-2. To simulate a wireless sensor network experiment we added Mannasim patches in to NS-2. Mannasim extends NS-2 by introducing new modules for design, development and analysis of different WSN applications. In order to experiment security and integrity features for wired, wireless and sensor network, we need to add combined security and integrity Agent into NS-2. The purpose of this project is only to illustrate a way to add security and integrity Agent into NS-2.

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. Within new derived class we will implement message digest generation function to ensure the integrity of data packet during transmission we will also add encryption and decryption for the modified data packet.

For development of this combined security and integrity agent in to NS-2 tool developer need following prerequisite

- Personal Computer with Ubuntu 12.04 or Cygwin with Windows 7
- NS- 2.35,
- Mannasim patches for Wireless Sensor Networks simulation
- C/C++ editor
- Programming skill: C++ and TCL

Procedure to Add a New Packet Protocol into NS-2:

Marc Greis's tutorial shows how to add a new packet protocol to NS-2 (Figure 1.1). The new packet class is created in the folder.../apps. After that, the new packet name has to register to the packet.h. Of course, the makefile has to be modified 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 file. Finally, we have to make an entry for the new packet in the ns-packet.tcl file. After recompile the ns-2, we can use the new packet for our simulation (P.Vijayakumar, *et al* 2010).

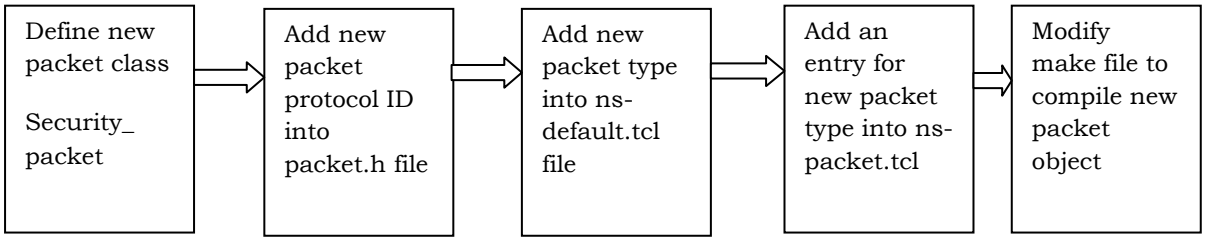

Fig. 1.1: shows how to add a new packet protocol to NS-2.

Packet Format:

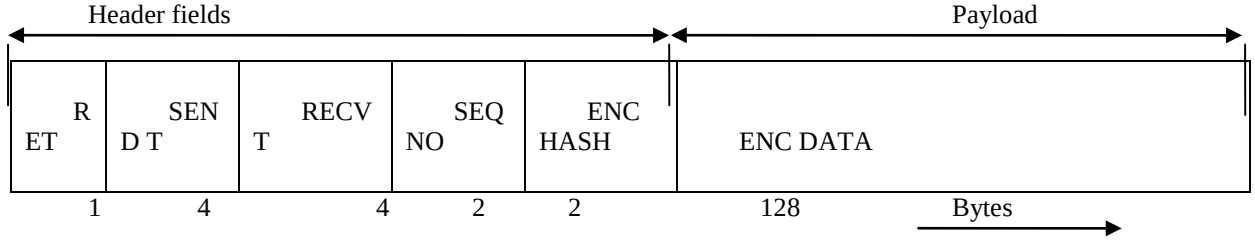

Fig. 1.2: shows modified packet format.

Figure 1.2 shows modified packet format.In modified packet format to achieve integrity of data transmission we added one extra field in the header for sending the encrypted hash value. In payload field we usually send plain text but here we are sending cipher text to achieve secure transmission. In addition with these it also contain some fields like RET, SEND T, RECV T and SEQ NO. In transmitting side sender set RET field to 0.In the receiving side the receiver receives that packet and it came to know that it has to generate an acknowledgement packet if the RET field is 0. SEND T and RECV T is used to calculate round trip time of the packet and SEQ NO is used reorder the packet in receiver side.

Design structure of combined of Security and integrity Agent:

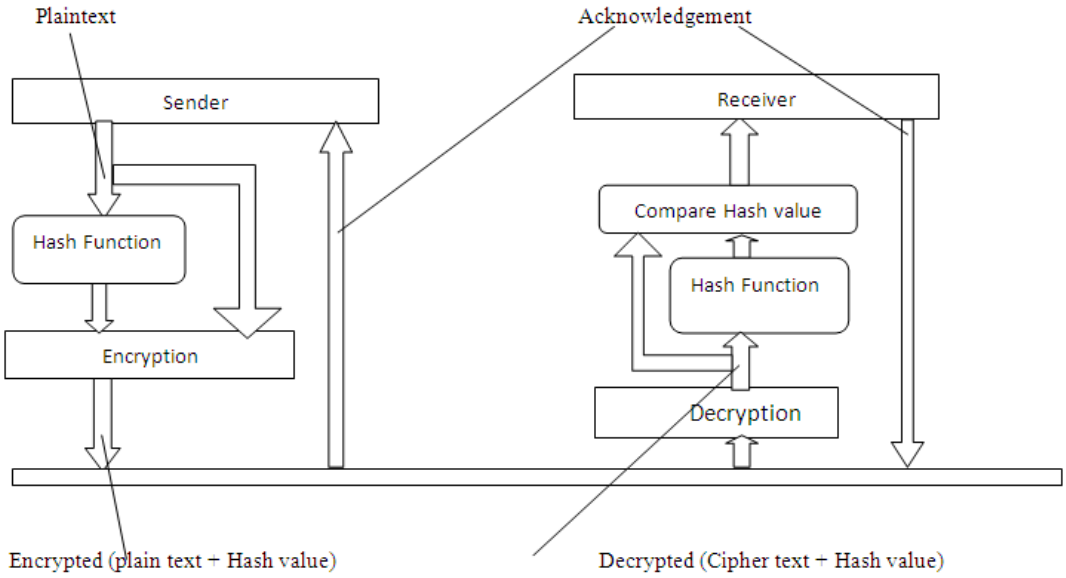

Fig. 1.3: shows the design of secure data and integrity of data transmission and reception system.

The design structure of secure and integrity of data transmission and reception system is shown in Figure 1.3. Sender: The sender is a device that sends data message. Plain text: An original data message is known as the plain text. Hash function: A hash function that maps a variable length data block or message in to a fixed length value called a hash code, hash value, hash sum, or simply hash. Encryption: The process of changing plain text into cipher text is called encryption. Cipher text: The encrypted form of message and hash value is called cipher text. Transmission medium: The transmission medium is the physical path by which a message travels from sender to receiver. Here medium are radio waves or wire. Decryption: The process of restoring plain text from the cipher text is called decryption Receiver: The receiver is a device that receive data message.

For WSN a simple Polynomial hash algorithm and for Wired and wireless network SHA-1 algorithm is used to obtain hash value from a string of plain text. Then the hash value is encrypted and the encrypted hash value will be attached to packet along with encrypted data for data integrity checking. At the other end of communication, after decryption, the decrypted text will be hashed again to get new hashed value. This new hashed value will be compared to the decrypted hash value attached within packet. If they are equal, the data integrity is ensured and decrypted text is accepted; otherwise the packet is discarded. In either case, an acknowledge packet will be sent back to sender to inform of the status of the packet. In WSN for encryption and decryption simple CESAR cipher algorithm is used and in Wired and wireless network RSA algorithm is used.

Algorithm:

SHA-1: The algorithm takes as input a message with a maximum length of less than 2^ 64 bits and produces as output of 160 bit message digest (William Stallings).

SHA-1 logic:

1. Pad message so its length is 448 mod 512
2. Append a 64-bit length value to message
3. Initialise 5-word (160-bit) buffer (A, B, C, D, E) to (67452301, EFCDAB89, 98BADCFE, 10325476, C3D2E1F0).
4. Process message in (512-bit) blocks:

- It consist of four round of processing of 20 steps each .the four round have similar structure but each use of different primitive logical function f1,f2,f3,f4.
- Each round takes as input the current 512 bit blocks being processed and 160-bit buffer value ABCDE and updates the content of buffer. Each round make use of additive constant K_t.
- The output of the fourth round added to the input of first round to produce CVq+1

5. After all 512-bits block have been processed output from L^{th} stage is 160 bit message digest.

SHA-1 Compression Function:

Each of 80 step processing of 512-bit performs given function.

(A, B, C, D, E)<- (E+f(t,B,C,D)+(A<<5)+W_t+K_t),A,(B<<30),C,D)

Here

- A, B, C, D refers to the 4 words of the buffer.
- t is the step number.
- f (t, B, C,D) is primitive logical function for round.
- W_t is derived from the message block from 512-message.
- K_t is an additive constant.

RSA:

1. RSA (Rivest, Shamir, Adleman) is the one of the most popular public key encryption (William Stallings).
2. The RSA scheme is a block cipher in which the plain text and cipher text are integer between 0 and n-1 for some value of n.
3. A typical size for n is 1024 bits or 309 decimal digits.

RSA Key Setup:

4. Each user generates a public/private key pair by for that Selecting two large primes at random p, q
5. Computing their system modulus N=p*q
   Note ø(N)=(p-1)(q-1)
6. Selecting at random the encryption key e
   Where 1<e<ø(N), gcd(e, ø(N))=1
7. Solve following equation to find decryption key d
   d*e=1 mod ø(N) and 0≤d≤N
8. Publish their public encryption key: KU={e, N}
9. Keep secret private decryption key: KR={d, N}

RSA Encryption/Decryption:

10. To encrypt a message M the sender obtains public key of recipient KU={e, N}
11. Computes: $C=M^e$ mod N, where 0≤M<N
12. To decrypt the cipher text C the owner uses their private key KR={d, N}
13. Computes: $M=C^d$ mod N

CESAR Cipher Encryption and Decryption:

The CEASER Cipher Encryption and Decryption algorithm which is implemented for WSN is to ensure security given below (P.Vijayakumar, *et al).*

```
void Security_packetAgent::encryption (char out[])
{
int key =3;
int i=0;
for (i=0;i<strlen(out);i++)
{
out[i]=(out[i]+key)%128;
}
}
```

```
void Security_packetAgent::decryption(char out[])
{
int key =3;
int i=0;
for (i=0;i<strlen(out);i++)
{
out[i]=(out[i]-key)%128;
}
}
```

Polynomial Hash Algorithm:

The polynomial hash algorithm implemented for WSN to ensure the integrity of data transmission is shown below (P.Vijayakumar, *et al)*.

```
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;
}
```

In this project we used the NAM window (figure1.4a&figure1.4b) to display the data transmission happening between sending and receiving node in a wired, wireless and sensor networks environment in the NS-2 tool. At the mean time we also used the terminal window to ensure secure and integrity of data transmission between the two nodes. The figure1.5a displays secure and integrity of data transmission in Wired and wireless networks. The figure1.5b displays secure and integrity of data transmission in WSN.

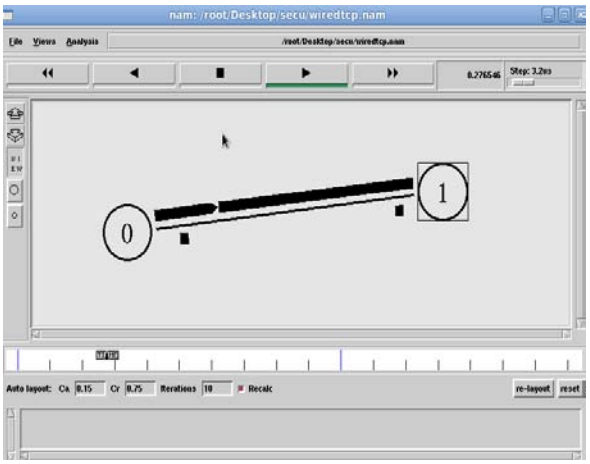

Fig. 1.4a: NAM displays packet transmission in wired network

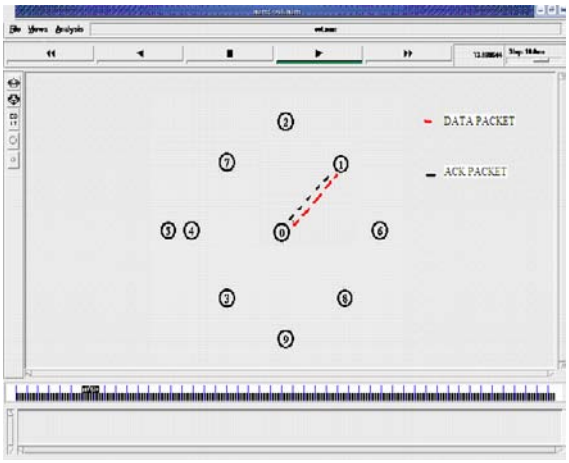

Fig. 1.4b: NAM Display packet transmission in Wireless and WSN

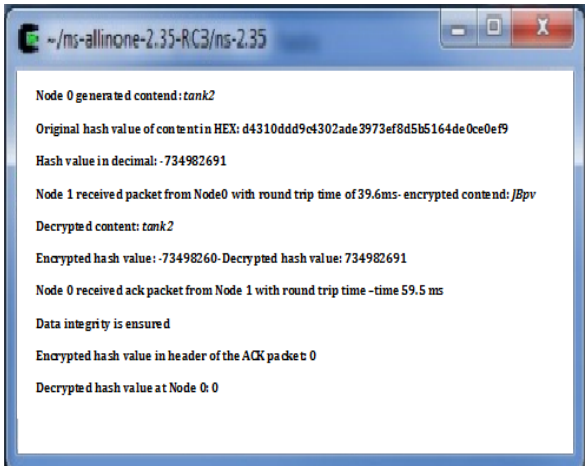

Fig. 1.5a: Terminal window displays secure and integrity of data transmission in wired network and Wireless network

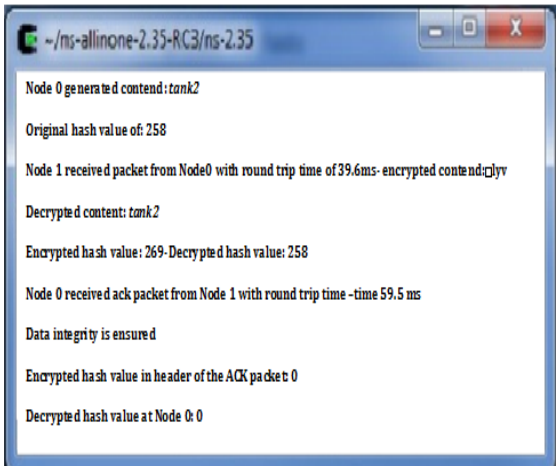

Fig. 1.5b: Terminal window displays secure and integrity of data transmission in WSN

Conclusion:

This project shown a method to add combined security and integrity Agent into NS-2 for wired ,wirerless and sensor networks by using existing one feasible instance encryption/decryption and hash algorithm . With this approach, we can built few more new combined security and integrity agent into NS-2 using algorithm such as SHA-256,SHA-384,SHA- 512 ,etc for hash function and DES, RC5,AES, etc for encryption / decryption. With this approach researcher can also add his or her own cobmined security and integrity Agent into NS-2 by introducing new encryption/decryption and hash algorithm.

REFERENCES

Book, A. William Stallings, 2013. Cryptography and Network Security, Sixth Edition, Prentice Hall, Part of the Pearson Custom Library, Computer Science series.

Erdal Cayirci and Chunming Rong, 2009."Security in Wireless Ad Hoc and Sensor Networks", A John Wiley and Sons, Ltd, Publication, pp: 119.

Hao Yang, Fabio Ricciato, Songwu Lu, and Lixia Zhang, 2006. "Securing a Wireless World", Proceedings of the IEEE, 94(2): 442-454.

Min-kyu Choi, Rosslin John Robles and Tai-hoon Kim1, 2008. "Wireless Network Security: Vulnerabilities, Threats and Countermeasures", International Journal of Multimedia and Ubiquitous Engineering, 3: 3.

Siddhartha Gupte and Mukesh Singhal, 2003. "Secure routing in mobile wireless ad hoc networks", Elsevier Ad Hoc Networks journal, 1(1): 151-174.

Vijayakumar, P. and C. Manikandan, 2010. "Security Function Integration into NS-2 for WSN", 2^{nd} National Conference on Information and Software Engineering.

Yong Wang, Garhan Attebury, and Byrav Ramamurthy, 2006. "A Survey Of Security Issues In Wireless Sensor Networks" , IEEE Communications Surveys & Tutorials, 8(2).