An Approach to Secure Hierarchical Network using Joint Security and Routing Analysis

Shivamalini L
M. Tech Research Scholar,
Department of CSE,
Dayananda Sagar College of Engineering, Bangalore, India.

Manjunath S S
M. Tech Research Scholar,
Department of CSE,
Dayananda Sagar College of Engineering, Bangalore, India.

ABSTRACT

In wired networks, building reliable and secured network connections is becoming extremely important. Security and Routing in wired networks remain challenging problem due to the complexity involved such as improper path discovery, congestion, network traffic and delay. In this paper, we first analyze the vulnerabilities for networks under different types of attacks. Then, we propose an Authentication and key assignment protocol to hierarchical routing to overcome those vulnerabilities with the security functionality to prevent malicious attacks. Hence, both Security and routing analysis is provided for Hierarchical Network Routing using Authentication and Integrity, and Key Assignment protocol. A class of continuous metrics to evaluate the vulnerability as a function of security and routing protocols used in networks has been formulated. Joint analysis of Security and Routing is used as it reveals the weaknesses in the network that remain undetected when Security and Routing protocols are analyzed independently. Interleaving has also been considered to increase performance. Performance metrics such as Packet Delivery Fraction, End-to-End Delay, and Packet Loss are considered.

General Terms

Authentication, Hierarchical Routing, Key Assignment and Vulnerability.

Keywords

Authentication, Attack, Hierarchical Routing, Key Assignment Protocol, Network Security, Routers, Vulnerability.

1. INTRODUCTION

Hierarchical Network Routing is a method of routing in networks based on hierarchical addressing. Hierarchical Routing was mainly devised to reduce memory requirements over large topologies. This topology is broken down into several Layers, thus downsizing the load on the routers. The router consists of routing table, the length of the routing table must be as small as possible and also the information that these routing table contains must be confidential from other routers. Hence, routers must ensure security. In networks, to secure the communication over the insecure communication channels is a big challenge. Therefore, the user Authentication and key assignment have become an important security service for communication networks A variety of protocols for authentication and key assignment which enable the users to be authenticated in order to get service from service provider have been proposed and applied to many existing communication systems. Kerberos [1] which works based on the technique of timestamp and symmetric secret key is one of the most widely used Authentication and key assignment protocols. However, it has drawbacks to suffer from the vulnerability under the password guessing attack, replay attack and exposure of session key. Many efforts have been devoted to improve its security, the scalability, and the efficiency [2]. There are also some formal methods applied to the analysis of Kerberos [3], [4]. In this article, we also introduce a class of metrics to measure the effective security offered in a network as a function of routing topology and the link security provided by the key assignment protocol. Hence, to achieve security to hierarchical network, Authentication and key assignment protocol has been proposed.

The major contribution made in this paper can be summarized as follows:

- We analyze *man- in-the-middle attack* in the hierarchical network and investigate the vulnerabilities caused by this attack.
- We define a class of continuous metrics to evaluate the vulnerability as a function of security and routing protocols.
- We propose a solution to prevent this attack using authentication and key assignment protocol.

The rest of this article is organized as follows. In Section 2, presents some related work in the area of security using key assignment and ensuring security to hierarchical network. In Section 3, different types of attacks are described. In Section 4, we propose our key assignment protocol and analyze its security in hierarchical network. Section 5 presents the simulation results carried out on the proposed mechanisms and Performance Metrics. Finally, we conclude this paper in Section 6. This is followed by Acknowledgement and References.

2. RELATED WORK

In recent years, many schemes have been proposed to secure the routing protocols against different attacks launched by malicious or compromised nodes. Sujata Doshi and Anand Eswaran [5] proposed hierarchical security architecture for group-communication in sensor networks. A secure architecture for bootstrapping sensor networks in which the sensor nodes form a hierarchy based on the strength of the composite key was proposed. A node higher in the hierarchy is more resilient to malicious attackers as compared to a node lower down the hierarchy. At each level of the hierarchy random key pre-distribution is deployed to create pair wise keys between nodes of the level. In addition unique keys are established between the parent nodes and the child nodes.

Mohammad O. Pervaiz, Mihaela Cardei, and Jie Wu [6] proposed routing security in Ad hoc wireless networks. They have proposed some routing protocols in Ad hoc wireless networks. Security services and challenges, Security attacks on routing protocols, Security mechanisms and Solutions for routing protocols in Ad hoc wireless networks have been proposed.

Seung Yi, Prasad Naldurg and Robin Kravets [7] proposed security-aware Ad hoc routing for wireless networks. A new routing technique called Security-Aware ad hoc Routing (SAR) that incorporates security attributes as parameters into ad hoc route discovery was proposed. SAR enables the use of security as a negotiable metric to improve the relevance of the routes discovered by ad hoc routing protocols.

Suraj Sharma and Sanjay Kumar Jena [8] proposed A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks. A number of secure and energy efficient hierarchical routing protocols such as SRPSN, LHA-SP, F-LEACH, SLEACH, SHEER etc for WSN was studied and analyzed.

Chris Karlof and David Wagner [9] proposed Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Proposed security goals for routing in sensor networks, show how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks — sinkholes and HELLO floods, and analyze the security of all the major sensor network routing protocols.

This paper proposes a method of ensuring security to hierarchical network routing using authentication and key assignment protocol. Hence, joint security and routing analyses used in hierarchical network reveals the weaknesses in the network that remain undetected when security and routing are analyzed independently.

3. TYPE OF ATTACKS IN NETWORK

i) ***Man-in-the-middle Attack:*** A man-in-the-middle (MITM) attack [10] is a kind of attack that an attacker makes independent connections with the victims and relays messages between them, making them believe that they are communicating directly to each other over a private connection whereas, in fact, the entire conversation is controlled by the attacker.

ii) ***Off-line Guessing Attack:*** An off-line guessing attack is also referred as off-line dictionary attack. This is a kind of attack that an attacker eavesdrops communication messages during the operation of a protocol and stores them locally. Then the attacker tries to find out the weak password by repeatedly guessing a possible password and verifying the correctness of the guess via the captured information in an offline manner. In order to prevent an off-line guessing attack, it is necessary to have a precise definition on it and a clear picture to reveal the potential vulnerabilities under the off-line guessing attacks.

iii) ***Misrouting Attack:*** In the misrouting attack, a non-legitimate node sends data packet to the wrong destination. This type of attack is carried out by modifying the final destination address of the data packet or by forwarding a data packet to the wrong next hop in the route to the destination.

iv) ***Detour Attack:*** In this type of attack, the attacker adds a number of virtual nodes in to a route during the route discovery phase. As a consequence, the traffic is diverted to other routes that appear to be shorter and might contain malicious nodes which could create other attacks. The attacking node can save energy in a detour attack because it does not have to forward packets to that destination itself. This attack is specific to source routing protocols.

v) ***Wormhole Attack:*** In the wormhole attack [11], two compromised nodes can communicate with each other by a private network connection. The attacker can create a vertex cut of nodes in the network by recording a packet at one location in network, tunneling the packet to another location, and replaying it there. The attacker does not require key material as it only needs two transceivers and one high quality out-of-band channel. The wormhole can drop packets or it can selectively forward packets to avoid detection. It is particularly dangerous against different network routing protocols in which the nodes consider themselves neighbor after hearing a packet transmission directly from some node.

vi) ***Tunneling Attack****:* In a tunneling attack [12], two or more nodes collaborate and exchange en- capsulated messages along existing data routes. For example, if a Route Request packet is encapsulated and sent between two attackers, the packet will not contain the path traveled between the two attackers. This would falsely make the receiver conclude that the path containing the attackers is the shortest path available.

4. PROPOSED METHOD

The purpose of our study was to provide security in hierarchical network routing. Many previous Hierarchical routing protocols assume a safe and secure environment where all nodes cooperate with no attack present. But the real world environment is totally opposite; there are many attacks that affect the performance of routing protocol. To overcome this we ensure security to hierarchical network using Authentication and key assignment protocol. Interleaving is considered too increase performance.

In the proposed method every node is assigned with a key. Every time the exchange of information takes place between the nodes, it authenticates and key should be matched. i.e.. When a sender node has to send information to the other end, then the server asks for a key, this key should be matched with the key assigned to that node initially. Only on success authentication the information exchange takes place. Similarly, when the information has to be routed to its lower nodes then a key is asked and the key should be matched with the assigned key. Hence, security is provided to the hierarchical network.

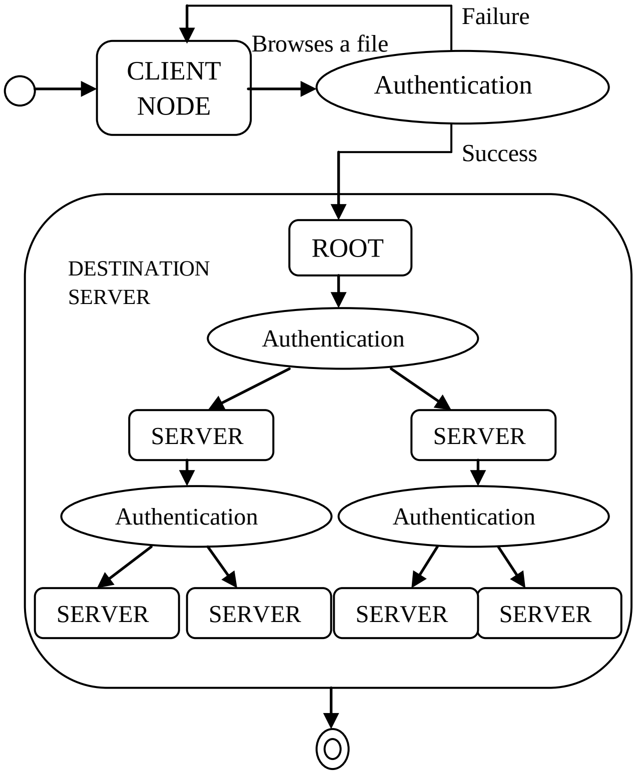


Fig 1: Block Representation of proposed hierarchical network with Authentication and Key assignment protocol.

A class of continuous metrics has been formulated to evaluate the vulnerability as a function of security and routing protocols used in networks.

The Classes of metrics are:

- The class of independent path routing protocols consists of any protocol which uses one or more paths to route separate messages such that messages traversing different paths are independently coded and secured.

- The class of dependent path routing protocols consists of any which uses multiple paths in which packets traversing separate paths are jointly coded, fragmented, or secured.

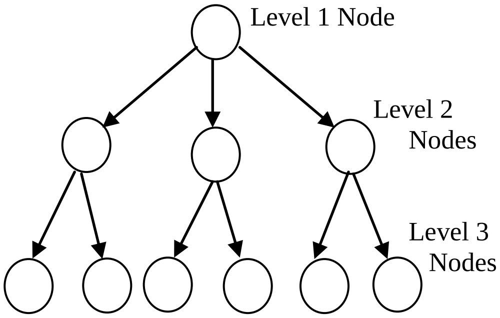


Fig 2: Node Hierarchy Structure.

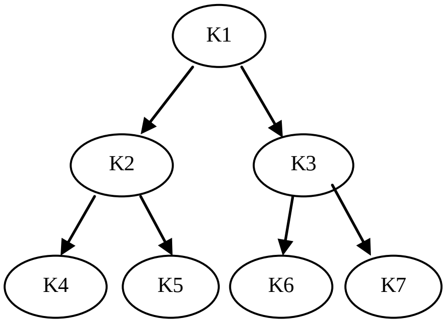


Fig 3: Logical Key Hierarchy.

Node hierarchy structure is shown in fig 2. In this diagram, each node can securely establish contact with any peer at its own level. Besides a node also has a unique key to communicate with its parent node at the immediately higher level. Logical key hierarchy is shown in fig 3. In this diagram, K1 is the common group key while the other keys are useful during routing messages to its peers. Each physical node corresponds to a leaf node in the Logical Key hierarchy. With the help of this Logical key the communication between peers takes place.

4.1 Joint Security and Routing Analysis with Interleaving

In this module, joint security and routing analysis module and interleaving module is combined to increase performance. The file is encoded using FEC and interleaved at the client side. While sending a key is asked for to authenticate the client and then sent to the destination. At the destination, a key is asked for; this key is matched with the client key. On success, the file is received at the destination. Then this file is de- interleaved and decoded. On click Result button, the file which is received is displayed and block rate, efficiency are calculated, and is shown in fig.3. At each node in the hierarchy the same process is continued.

The performance of FEC coding is evaluated more accurately. The unified approach provides an integrated framework for exploring the tradeoffs between the key coding parameters: specifically, Interleaving depths, channel coding rates and block lengths. Thus by choosing the coding parameter appropriately we have achieved high performance of FEC, reduced the time delay for Encoding and Decoding with Interleaving.

FEC is a system of error control for data transmission, where the sender adds redundant data to its messages. This allows the receiver to detect and correct errors (within some bounds) without the need to ask the sender for additional data. In this module we add redundant data to the given input data, known as FEC Encoding.

Interleaving is a way of arranging data in a non-contiguous way in order to increase performance. It is used in data transmission to protect against burst errors. In this module we arrange the data (shuffling) to avoid burst errors which is useful to increase the performance of FEC Encoding.

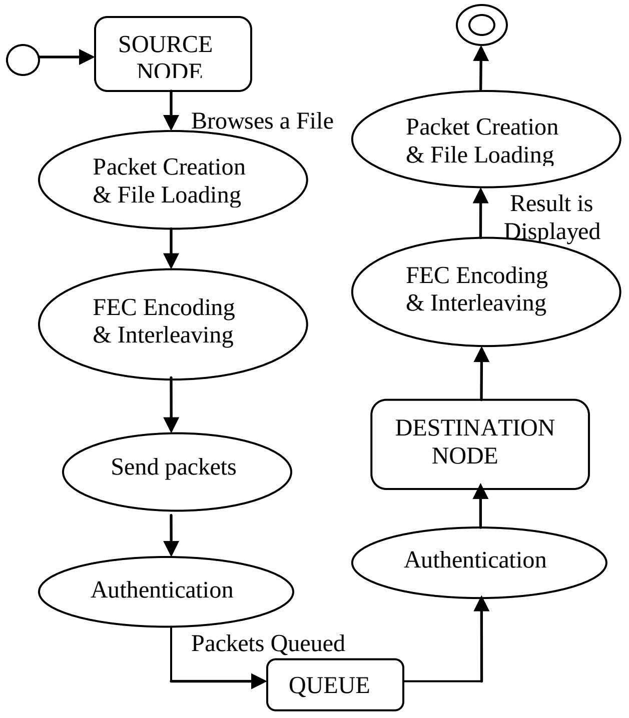


Fig 4: Logical Key Hierarchy.

The performance of FEC coding is evaluated more accurately. The unified approach provides an integrated framework for exploring the tradeoffs between the key coding parameters: specifically, Interleaving depths, channel coding rates and block lengths. Thus by choosing the coding parameter appropriately we have achieved high performance of FEC, reduced the time delay for Encoding and Decoding with Interleaving.

FEC is a system of error control for data transmission, where the sender adds redundant data to its messages. This allows the receiver to detect and correct errors (within some bounds) without the need to ask the sender for additional data. In this module we add redundant data to the given input data, known as FEC Encoding.

Interleaving is a way of arranging data in a non-contiguous way in order to increase performance. It is used in data transmission to protect against burst errors. In this module we arrange the data (shuffling) to avoid burst errors which is useful to increase the performance of FEC Encoding.

Steps for FEC Encoding and Interleaving:

1. The contents of the file are changed to ASCII values, and this is converted to binary values.
2. These binary values are separated and additional two bits are added.
3. These bits are arranged without spaces.
4. Then the bits are shuffled and sent
5. At the destination, the reverse process takes place.

Example for showing FEC Encoding and Interleaving:

Ex: Hello

H: 72 → 1001000 → 1 0 0 1 0 0 0 0 → 111 000 000 111 000 000 000 000 → 1110000001110000000000 → 1 1 1 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0

Shuffled packet: 001101001 10000000100

e: 101 → 1100101 → 1 1 0 0 1 0 1 → 111 111 000 000 111 000 111 → 111111000000111000111 → 1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 0 0 0 1 1 1

Shuffled packet: 100000111111100100111

l: 108 → 1101100 → 1 1 0 1 1 0 0 → 111 111 000 111 111 000 000 → 111111000111111000000 → 1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0

Shuffled packet: 111101 01110100100101

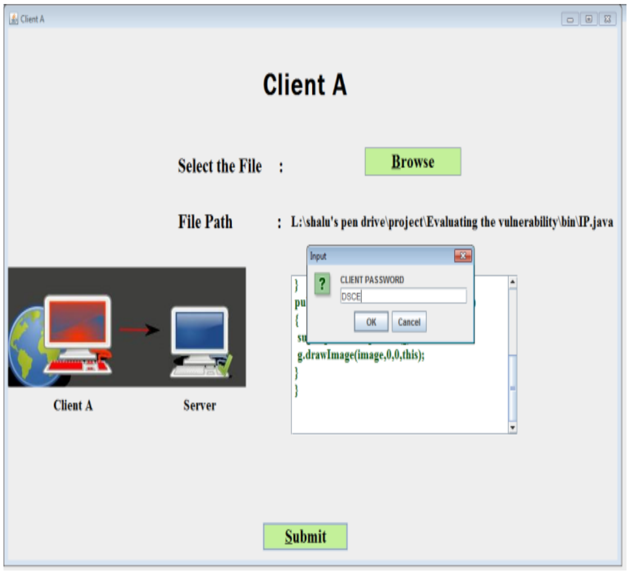
l: 108 → 1101100 → 1 1 0 1 1 0 0 → 111 111 000 111 111 000 000 → 111111000111111000000 → 1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0

Shuffled packet: 111101 01110100100101

o: 111 → 1101111 → 1 1 0 1 1 1 1 → 111 111 000 111 111 111 111 → 111111000111111111111 → 1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1

Shuffled packet: 111101011111101111111

Simulation has been done in Java language. The graphical user interfaces developed have been presented in the Figures below.


Client A

Select the File : Browse

File Path : L:\shalu's pen drive\project\Evaluating the vulnerability\bin\IP.java

Input

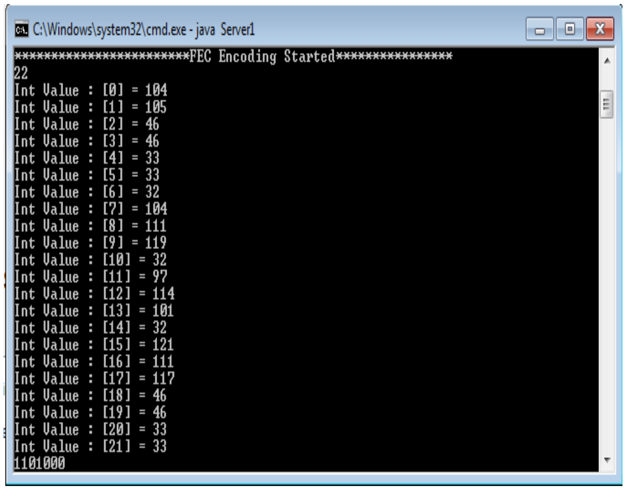
CLIENT PASSWORD

DSCE

OK Cancel

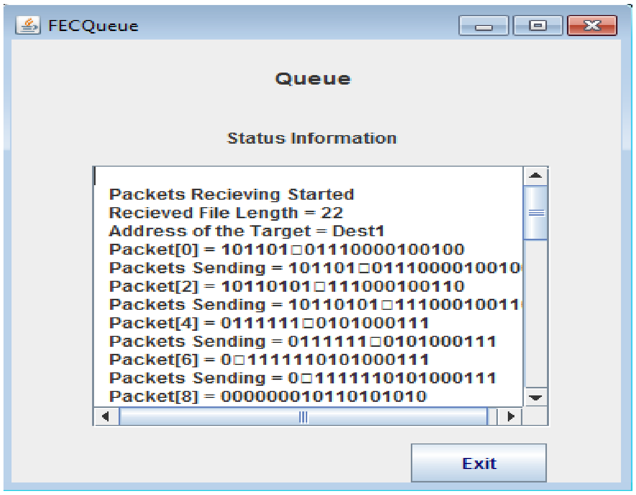
```
}
pu
{
 su
 g.drawImage(image,0,0,this);
}
}
```

Fig 5: Browses for a File and Client's Password is Asked.



```
C:\Windows\system32\cmd.exe - java Server1
************************FEC Encoding Started****************
22
Int Value : [0] = 104
Int Value : [1] = 105
Int Value : [2] = 46
Int Value : [3] = 46
Int Value : [4] = 33
Int Value : [5] = 33
Int Value : [6] = 32
Int Value : [7] = 104
Int Value : [8] = 111
Int Value : [9] = 119
Int Value : [10] = 32
Int Value : [11] = 97
Int Value : [12] = 114
Int Value : [13] = 101
Int Value : [14] = 32
Int Value : [15] = 121
Int Value : [16] = 111
Int Value : [17] = 117
Int Value : [18] = 46
Int Value : [19] = 46
Int Value : [20] = 33
Int Value : [21] = 33
1101000
```

Fig 6: FEC Encoding and Interleaving Starts.



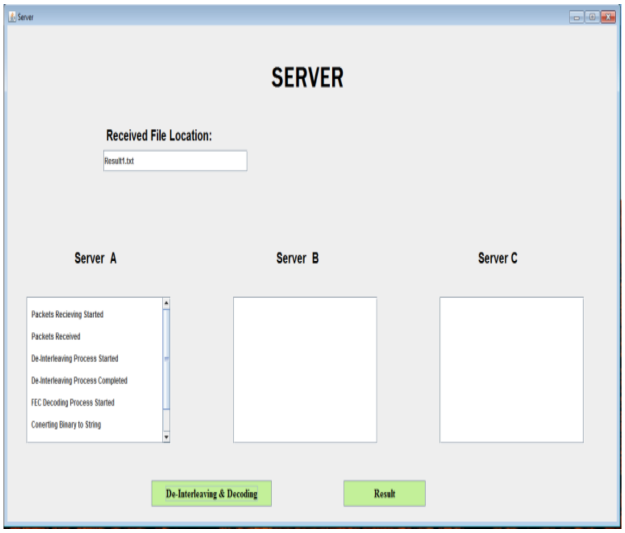
FECQueue

Queue

Status Information

```
Packets Recieving Started
Recieved File Length = 22
Address of the Target = Dest1
Packet[0] = 101101□01110000100100
Packets Sending = 101101□0111000010010
Packet[2] = 10110101□111000100110
Packets Sending = 10110101□11100010011
Packet[4] = 0111111□0101000111
Packets Sending = 0111111□0101000111
Packet[6] = 0□1111110101000111
Packets Sending = 0□1111110101000111
Packet[8] = 000000010110101010
```

Fig 7: Packets are Queued.



SERVER

Received File Location: Result1.txt

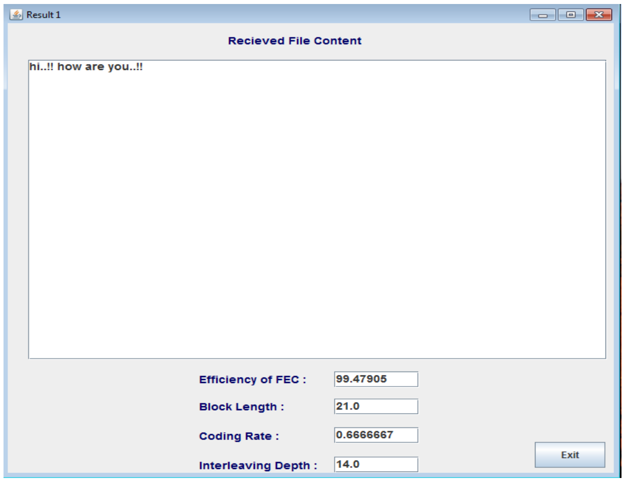
Server A

Server B

Server C

Packets Recieving Started
Packets Received
De-Interleaving Process Started
De-Interleaving Process Completed
FEC Decoding Process Started
Conerting Binary to String

Fig 8: Server Side: De-Interleaving and Decoding takes place.



Result 1

Recieved File Content

hi..!! how are you..!!

Efficiency of FEC : 99.47905

Block Length : 21.0

Coding Rate : 0.6666667

Interleaving Depth : 14.0

Fig 9: Received file content which calculates the efficiency, coding rate and interleaving depth.

5. EXPERIMENTAL RESULTS

The proposed method has been implemented on network simulator ns-2 [13] to evaluate the performance and to show the statistics. The nodes were created in a hierarchical manner and duplex links are created in order to connect nodes. The type of link is specified for each node. When simulation starts, the data flows hierarchically from root to the other nodes. The simulation is shown using NAM. The trace file is generated.

The trace file contains the following: Event, Time, From, To, Type, Size, Flags, Class, Source, Destination, Sequence, and Identifier.

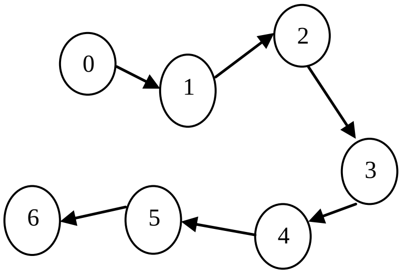


Fig 10: Network Topology Simulated in NS-2.

Table 1 shows the trace file that is generated when the simulation for hierarchical routing is run.

5.1 Performance Metrics

Three performance metrics are focused which are quantitatively measured. The performance metrics are important to measure the performance. The performance metrics are [16]:

i) Average end-to-end delay of data packets — there are the possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times. Average end-to-end delay is an average delay of data packets. It is also caused by queuing for transmission at the node and buffering data for detouring. Once the time difference between every CBR packet sent and received was recorded, dividing the total time difference over the total number of CBR packets received gave the average end-to-end delay for the received packets. This metric describes the packet delivery time; the lower the end-to-end delay the better the application performance.

Table 1: A Part of the Trace File.

Event	Time	From	To	Type	Size	Flags	Class	Source	Destination	Sequence	Identifier
+	1	0	1	cbr	210	-----	0	0.0.0.0	1.1.1.0	0	0
-	1	0	1	cbr	210	-----	0	0.0.0.0	1.1.1.0	0	0
r	1.002336	0	1	cbr	210	-----	0	0.0.0.0	1.1.1.0	0	0
+	1.002336	1	5	cbr	210	-----	0	0.0.0.0	1.1.1.0	0	0
-	1.002336	1	5	cbr	210	-----	0	0.0.0.0	1.1.1.0	0	0
+	1.00375	0	1	cbr	210	-----	0	0.0.0.0	1.1.1.0	1	1
-	1.00375	0	1	cbr	210	-----	0	0.0.0.0	1.1.1.0	1	1
r	1.004672	1	5	cbr	210	-----	0	0.0.0.0	1.1.1.0	0	0
+	1.004672	5	6	cbr	210	-----	0	0.0.0.0	1.1.1.0	0	0
-	1.004672	5	6	cbr	210	-----	0	0.0.0.0	1.1.1.0	0	0
r	1.006086	0	1	cbr	210	-----	0	0.0.0.0	1.1.1.0	1	1
+	1.006086	1	5	cbr	210	-----	0	0.0.0.0	1.1.1.0	1	1
-	1.006086	1	5	cbr	210	-----	0	0.0.0.0	1.1.1.0	1	1
r	1.007008	5	6	cbr	210	-----	0	0.0.0.0	1.1.1.0	0	0
+	1.007008	6	7	cbr	210	-----	0	0.0.0.0	1.1.1.0	0	0
-	1.007008	6	7	cbr	210	-----	0	0.0.0.0	1.1.1.0	0	0
+	1.0075	0	1	cbr	210	-----	0	0.0.0.0	1.1.1.0	2	2
-	1.0075	0	1	cbr	210	-----	0	0.0.0.0	1.1.1.0	2	2

Throughput -The ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet is referred to as throughput. It is expressed in bits per second or packets per second. Factors that affect throughput include frequent topology changes, unreliable communication, limited bandwidth and limited energy. A high throughput network is desirable.

ii) Packet delivery fractions (PDF) — the ratio of the data packets delivered to the destinations to those generated by the CBR sources. The PDF shows how successful a protocol performs delivering packets from source to destination. The higher for the value give use the better results. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol by giving its effectiveness.

iii) Data Packet Loss (Packet Loss) — Mobility-related packet loss may occur at both the network layer and the MAC layer. Here packet loss concentrates for network layer. When a packet arrives at the network layer, the routing protocol forwards the packet if a valid route to the destination is known. Otherwise, the packet is buffered until a route is available.

A packet is dropped in two cases:

- Buffer is full.
- Buffer time is exceeded.

6. CONCLUSION

In this paper, security has been implemented in the hierarchical network using Authentication and key assignment protocol. Hence, joint analysis of security and routing is achieved in hierarchical network. Key is provided at every node in the hierarchy and thus providing security. Hence, a method has been proposed to secure the data while routing, using Authentication which is similar to simple password scheme and key assignment in which keys are accepted dynamically from source and sink is matched. Based on this matching, the data is routed hierarchically. Authentication and key assignment protocol to hierarchical network was designed to overcome vulnerabilities in the network with the security functionality to prevent malicious attacks. Finally, we investigated the problem of developing vulnerability metrics that improve the efficiency when routing and key assignment protocols used in the networks are jointly analyzed.

Performance metrics such as end-to-end delay, packet delivery fractions and packet loss has been considered. End-to-end delay is measured by considering the time taken to deliver the packets completely and successfully. Packet loss occurs due to the buffer overflow or congestion and is implemented using drop tail in NS2 and packets are dropped when the traffic is more in the network. Packet loss is avoided by proper provisioning of link capacities and retransmission of packets.

7. ACKNOWLEGEMENT

This paper would not have existed without my guide Asst. Prof. Manjunath S.S. I also would like to thank our head of the department Dr. D. R. Ramesh Babu, Prof. Bhaskar Rao and my colleague Surya.S.Raju.

8. REFERENCES

[1] J.Kohl and C.Neuman, "RFC 1510: The Kerberos Network Authentication Service (V5)," Sep.1993.

[2] H.-Y. Chien and J.-K. Jan, "A hybrid authentication protocol for large Mobile network," *The Journal of Systems and Software*, vol. 67, no. 2, pp. 123–130, Aug. 2003.

[3] G. Bella and E. Riccobene, "Formal analysis of the Kerberos authentication system," *Journal of Universal Computer Science*, vol. 3, no. 12, pp. 1337–1381, Dec. 1997.

[4] A. Scedrov, F. Butler, A. D. Jaggard, and C. Walstad, "Formal analysis of Kerberos 5," *Theoretical Computer Science*, vol. 36, no. 1–2, pp. 57–87, Nov. 2006.

[5] Sujata Doshi and Anand Eswaran, "A Hierarchical Security Architecture for Group-Communication in Sensor Networks".

[6] Mohammad O. Pervaiz, Mihaela Cardei, and Jie Wu, "Routing Security in Ad Hoc Wireless Networks," Network Security Scott Huang, David MacCallum, and Ding Zhu Du(Eds.), 2005.

[7] Seung Yi, Prasad Naldurg and Robin Kravets, "Security Aware Ad hoc routing for Wireless Networks".

[8] Suraj Sharma and Sanjay Kumar Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," *ICCCS'11* February 2011.

[9] Chris Karlof and David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures".

[10] Zhe Chen, Shize Guo, Kangfeng Zheng and Yixian Yang, "Modeling of Man-in-the-Middle Attack in the Wireless Networks," 2007 IEEE.

[11] Y. -C. Hu, A. Perrig, and D. B. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, Infocom 2003.

[12] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, A Secure Routing Protocol for Ad hoc Networks, The 10th IEEE Intl. Conf. on Network Protocol (ICNP), Nov. 2002.

[13] NS-2 Simulator. URL:http://www.isi.edu/nsnam/ns.

[14] Chao Lv, Maode Ma, Hui Li and Jianfeng Ma, "A Security Enhanced Authentication and Key Distribution Protocol for Wireless Networks," 2010 IEEE.

[15] Patrick Tague, David Slater, Jason Rogers and Radha Poovendran, "Evaluating the Vulnerability of Network Traffic Using Joint Security and Routing Analysis," IEEE 2009.

[16] Huaizhi Li, Zhenliu Chen, Xiangyang Qin, Chengdong Li and Hui Tan, "Secure Routing in Wired Networks and Wireless Ad Hoc Networks, April 2002", Department of Computer Science, University of Kentucky.