Secure Transmission Against Packet Dropping Attack in Wireless Network using CPHS

K. Amuthapriya, P. Dhivyabharathi
Department of CSE,
SriVidya College of Engineering &Technology.
Virudhunagar.

M. Mohana (M.E-CSE)
Assistant Professor of Department of CSE ,
SriVidya College of Engineering
&Technology,Virudhunagar.

***Abstract*: Mobile ad hoc network is a wireless network that transmits input from one computer to another computer. Instead of using a central access point to which all computers must communicate, this peer-to-peer mode of operation can greatly extend the distance of the wireless network. We now focus on attacks against the routing protocol in ad hoc networks. DoS -Denial of service attack is an incident in which the user or organization is deprived of the services of a resource they would normally expect to have these attacks may have the aim of modifying the routing protocol so that the traffic flows through a specific node controlled by an attacker. Here interested in determining whether the losses are caused by link errors and malicious drop. We present a packet hiding scheme based on Cryptographic puzzles. Cryptographic puzzles which employ computationally efficient cryptographic primitives, which are used to implement CPHS.**

Keywords: Attacks, CPHS, Wireless network, Denial-of-Service.

INTRODUCTION

Wireless network is highly sensitive to denial of service (DoS) attacks.Denial of Service (DoS) attack is an attack with purpose of preventing legitimate users from using a specified network resources such as a websites, web services. The wireless communication channel is a broadcast medium, exposing the physical layer of wireless communication to jamming. An adversary can easily mask the events that the sensor network should detect by stealthily jamming an appropriate subset of the nodes. Any node under attack in ad hoc network show an anomalous behavior called the malicious behavior. anomalous behavior called the malicious behavior This malicious behavior cause disturbance in the network and to preclude such malicious behavior several security solutions have been discovered. In this paper, the malicious behavior of a node is defined and to defend such behavior, security solutions are presented which are used to provide secure and reliable communication in ad hoc network.

Here we present a packet hiding scheme based on Cryptographic puzzles. The main idea behind such puzzles is to force the recipient of a puzzle to execute a pre-define set of computations before he is able to extract a secret of interest. The time required for finding the solution of a puzzle depends on its hardness and the computational ability of the solver. The advantage of using puzzle based hiding scheme is that its security does not rely on the Physical layer parameters. However, it has higher communication and computation overhead. We consider several puzzle schemes as the basis for CPHS. We analyze the implementation details of each scheme which impact security and performance.

RELATED WORK:

Radhika Saini, Et al-To define the malicious behavior [1] of a node and define such behavior Security solution for a reliable communication malicious behavior of node is defined. Security solution to defend such behavior is provided. When a node under any attack and is therefore breaches any of the security principles . Such nodes exhibit one or more of the following behavior: Packet Drop, Packet Drop, Buffer Overflow etc. There are several security solutions which are used in ad hoc network. Security solutions can be provided through the methods of Cryptography, Protocols, Intrusion Detection System (IDS) and Trusted Third Party (TTP).

Jorvekar Priti Prakash et al :Puzzle based Autonomous encoding system provide a solution to selective [2] jamming attacks in the wireless network. This system provide facilities like encoding of packet, packet Interleaving, and puzzle based hiding system which Provide more secure packets. AES algorithm a security symmetric algorithm which is added for improving

security. It Provides extra security which not relies on PHY layer but it will cost computation cycles. Puzzle based scheme allows to hide packets temporarily at the time of transmission packets are encrypted randomly with AES and puzzles is send to the receiver for an attackers this puzzle is not able to solve so he is able to select packets and not able to generate selective jamming attacks

Rashmi B.Dhamannavar et al: In this model client can send data to server and server receive the data in a secure manner. We studied the preventive jamming attacks under two special cases.They are Cryptographic Puzzles, Strong Hiding [3] Commitment Schemes. The jammer is a part of the network under attack, thus being aware of the protocol specifications and shared network secrets. To avoid packet classification in wireless transmission we proposed two schemes such as commitment scheme based on strong hiding and hiding based on the cryptographic puzzle. These two schemes prevent the jammer from blocking the packets that are transmitted over the wireless network so that the data reaches the receiver without any inaccuracies.

Tao Shu et al: Nodes can cooperate in relaying and routing traffic in a multi-hop wireless network. An adversary can exploit this cooperative nature to launch attacks .A malicious node in the route can exploit its knowledge of the network protocol and the communication context to introduce an insider attack. That attack is intermittent. Detecting selective packet dropping attacks is extremely challenging in a highly changing wireless environment. We develop an accurate algorithm for detecting selective packet drops made by insider attackers. Our algorithm also provides a truthful and publicly verifiable decision or solution statistics as a proof to support the detection decision.

J. Karthikeyan et al: Packet may loss in the network due to a frequent link failure in ad hoc network. In this paper, we maintain log record at each router that record is used to find out where the loss actually occur and a special scheme used is Signal Stability- Based Adaptive routing protocol to find stable route during link failure. This protocol is beacon-based, in which the beacon signal strength is measured for determining link stability. The node then selects the alternate route to forward the packets without any loss. The significant nodes are assumed and implemented by using beacons count of the previous node. This model finds more stable routes to reduce path breaks and ill effects. If any loss of packet in network, the log record helps to detect where the loss in packet occurred and it can be recovered by Signal Stability-Based Routing.

Sruthy R.S. et al: Now a days internet is extremely affected by several attacks such as Denial-of-Service attacks.[6] The source IP address In a packet can be falsified. With the aim of ensuring a Total security, a Cryptographic puzzle based scheme is also combined with the new approach for preventing Hackers. Here certain puzzles are also used for encrypting the message along with the available methodologies. Here the opponent cannot solve the puzzle until the encrypted packet reaches the destination .The scheme is implemented based on a share market- based application. The security of the scheme is also analyzed. IP trace back based on DSA algorithm is less complex approach in tracing the source IP of a packet, here the secrecy of the transmitted data is achieved using Digital Signature Algorithm (DSA), the encrypted data transferred from source to destination is marked at the upcoming routers in the path. Thereby on fetching the information from the table the trace path can be reconstructed to analyze the source IP.

Lu Han et al: Wireless Mobile Ad-hoc Network is a collection of two or more devices connected with wireless communications and networking capability. These nodes can communication with other nodes that immediately within their radio range or outside their radio range. For later, the nodes needs to deploy an intermediate node to be the router to route the packet from the source to destination. The Wireless Ad-hoc Networks do not have a gateway; every node can act as the gateway. Even the most zealot supporters of MANET have to admit that it is a challenging task to enable fast and reliable communication within such a network. Mobile Ad hoc Networks are an ultimate technology to establish in an instant communication infrastructure less for military application. As we have proved using the three main technical topics of the Wireless Adhoc Networks,that the Ad-hoc Networks hold a flawed architecture for the following technical reasons:

The most important object for the networks is security. It is even important for Wireless Ad hoc Networks. Since its applications are in the military. The MANET cannot properly solve the problem of the secure Routing is also a big problem in MANET. All the routing protocols for Wireless Ad hoc Networks are need patches. Energy consumption problem of wireless networks still cannot be solved.

B. Mahalakshmi et al: Wireless networks are computer networks that are not linked or connected by cables of any kind. It enables the wireless connectivity to the Internet via radio waves. So it is more sensitive to the Denial-of-Service attacks. This paper contain information about Strong Hiding Commitment schemes, Cryptographic Puzzles Hiding Schemes, and wormholes for sending the message in wireless network securely even if the attacker is present and also alerts the other nodes about the presence of a jammer. Thus, it improves the performance and reliability of the router interface information is then logged into the table. Wireless sensor Network. A solution to the selective jamming attack in the wireless network would be the encryption of packet that is going to send. Here the encryption is applied to the attributes except destination. It means that we hide the packet from an attacker. The encryption is applied only to the attributes except destination. That is why during broadcasting there is no need for intermediated encryption. Each node checks the IP

address of an incoming packet. If it is sent to that particular node it will decrypt otherwise just forwarded to the next node. The problem of jamming under an internal threat model has been considered. An adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network has been designed.

Aejaz Ahmed et al: There are two sources for packet loss i.e. link error and malicious packet dropping. It is important to find whether the losses are only due to link errors or is due to both link error and malicious packet drop. Here, I am mainly interested in the insider attack case where malicious nodes drop packets selectively to degrade the network performance. Packet dropping rate in the insider attack case is nearly equal to normal link error because of which existing algorithms cannot find the exact cause of the packet loss. The main challenge here is for the guaranty of the information sent by the nodes to the auditor. The attacker usually sends the wrong information not to get detected. Sometimes the malicious node may drop the packet and will send that that the packet is transmitted. To overcome this problem we are using Homomorphic linear Authenticator (HLA) a cryptographic method which is used in cloud computing.

Felipe Perrone et al: In this paper, we formalized a common attack model on wireless networks which involve the combination of cyclical On and off processes. The attacks we considered are such that they experience an on-period, in which they actively seek to disrupt the operation of current running network, followed by an off period, in which the network experiences a transient due the adaptation mechanisms are built into its protocols.

PROPOSED SYSTEM

A solution to the selective attack on the wireless network would be the encryption of packet that is going to send. In wireless Ad Hoc Network, the data is sent using cryptography. Cryptography means to convert (or encrypt) the original data (which is to be sent) into the unreadable format. Even if the intruder accesses the data, it should not be able to understand the content of it. This security preserves the integrity and confidentiality of data. With the aim of ensuring a Total security, a Cryptographic puzzle based scheme is also incorporated along with the new approach for preventing Hackers and certain puzzles are also used for encrypting the message along with the available methodology. Here the attacker cannot solve the puzzle until the encrypted packet reaches the destination. Share market-based applications are base for implementing this scheme. The security of the scheme is also analyzed. Where a client can send data to server and server receive the data in a secure manner. When a sender wants to send a data to the receiver, the sender encrypts the data and sends in a secure manner by using Cryptographic Puzzle Hiding Scheme.

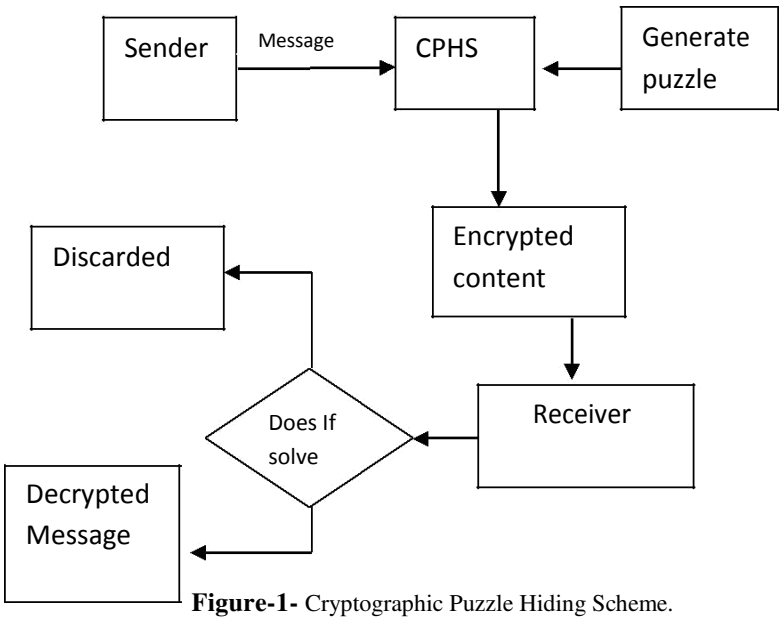

Figure-1- Cryptographic Puzzle Hiding Scheme.

A.Network Setup:

The network consists of a collection of nodes or devices connected via wireless links. Nodes may communicate indirectly through multiple hops , or directly if they are within communication range. Each node dragged from an edge of the network and it placed in the network area. After set the node, the location of the node get showed in IP text box. The communication flow starts when source decides to send messages to a client. It chooses a file and breaks it into many packets of size 48 bytes each and sends them to a randomly selected centralized server. There will be many numbers of nodes which we need to be added. Each node will be having a particular range to transmit the data.

B. Attack Occurrence:

Attackers which attack the transmission of specific packets. When data is sent from source to destination through Wireless Ad hoc Network. It can analyze the attacks and also find whether the attack is made or not. It is assumed that due to attack in sending packets may occur and in turn, it results in data loss or packet loss. The node can purposely drop packet is an attack.

C.Cryptographic Puzzle Hiding Scheme(CPHS): The purpose of a source is to send the data to the destination. The sender will be consisting of the Channel Encoder, Interleaver.

C.1) Encoder: Channel encoding deals with error control during the transmission through the communication channel. It expands the original bit sequence by adding necessary redundancy for protecting against channel errors .Here the sender adds redundant data to its messages. This allows the receiver/destination to detect and correct errors without the need to ask the sender for additional data. In this module, we add given input data with redundant data , known as Encoding. The text available in the input/source text file is converted into binary. The binary conversion is done for each and every character in the input file.Then we add each bit of the binary with redundant data.

C. 2) Interleaver: Interleaving is a way of arranging data in a non-contiguous order to increase performance. It is used in data transmission to protect against burst errors. In this the module we arrange the data (shuffling) to avoid burst errors This is useful to increase the performance of Encoding. This module gets the input as blocks of bits from the Encoder. In this module, we shuffle the bits inside a single block. This shuffling process is done for each and every block comes from the Encoder.

D.Affirmatory Phase:

Sending the packets from source to destination in a queue format i.e., first come first served the packets which come first will be sent first in a sequential order. It acts as a server which is used for identifying the destination and check the size of the data when we are transmitting. Each packet will be storing its corresponding information in the binary(0s and 1s) format. The packet hiding queue is responsible for sending the data to destination.

E .End To End Packet Delivery:

The destination will receive the path from where it can get the data from the packet hiding queue. The Destination will be consisting of the De-interleaver and Channel Decoder. At the receiver end, the interleaved data is arranged back into the original data by the de -interleaver. As a result, of interleaving, correlated noise introduced in the transmission channel appears to be statistically independent of the receiver and thus allows better error correction.

E.1)De–Interleaver: This module receives the blocks In error-correction coding, particularly within disk storage,memory,and data transmission. After interleaving, the data is converted into packets. Then the packets are used for the transmission. Identify the destination and data are converted into the packets and send to selected destination.

E.2) Decoder: The input for this module is De -Interleaved data. The received packets are processed to recover the original bits from it. In this module , we recover the original bits of a character. After receiving the original bits, we convert it into characters and write it into a textfile.

Performance analysis:

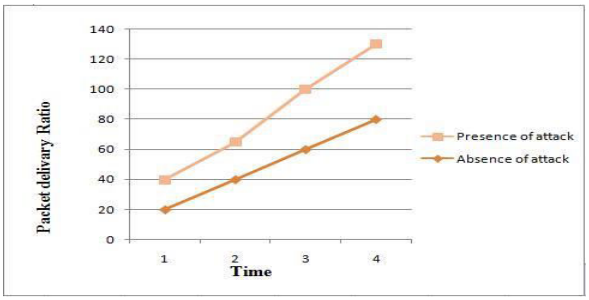

Figure-2:CPHS method analysis

Figure-2 graph is used to determine packet delivery ratio Vs time. If the attack is present in the path the packet delivery ratio will be very much decreased. The attack is not present in the path or The path has no attack the packet delivery ratio will be increased.

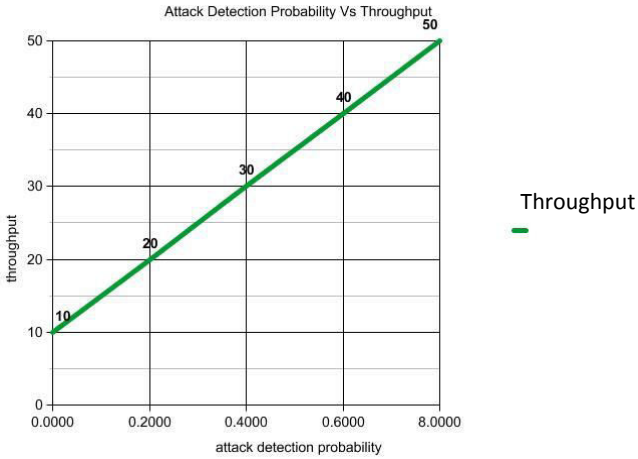

Figure-3 Through put

Throughput is the amount of packets received by the destination node over a period of time. Here the graph is used to determine the attack detection probability Vs Throughput. As the attack detection, the probability increases throughput also increases. The attack detection probability decreases throughput also decreases.

CONCLUSION:

In this paper, we address the problem of selective attack on the wireless ad-hoc network under an internal threat model, where the attacker is part of the network, who is aware of network secrets and also the implementation details. In order to overcome these kinds of attacks, we proposed new scheme: Cryptographic Puzzle Hiding Scheme (CPHS) which prevents an attacker from real-time packet classification. We can achieve the higher throughput by analyzing the comparative study of these schemes.

REFERENCES:

1. Radhika Saini And Manju Khari,- Defining Malicious Behavior Of A Node And Its Defensive Methods In Ad- Hoc Network, Volume 20– No.4, April 2011
2. .Jorvekar Priti Prakash, Gunjal Baisa L, Manish Gang want- " Puzzle-Based Packet Encoding Technique For Preventing ced Jamming Attacks In Wireless Network", International Journal OfEmerging Technology And Advan Engineering; Pp 2250 2459- July- 2013.
3. Rashmi B.Dhamannavar1, Dr.Rashmi M.Jogdand "Encryption Techniques In Packet-Hiding Methods To Prevent Jamming Attacks In Wireless Network", *International Journal Of Computer Science And Information Technologies*; Pp 4981-4985-2014.
4. Tao Shu And Marwan Krunz, Fellow, "PrivacyPreserving And Truthful Detection Of Packet Dropping Attacks In Wireless Ad HoNetworks",*Ieee Transactions On Mobile Computing*; April-2015.
5. J. Karthikeyan, Ashok Paranjothi "Detecting And Recovering Link- Failure In Ad-Hoc Network Using Signal Stability-Oriented Routing Protocol", *Article* · APRIL 2013
6. Sruthy R.S; "A Secure Cryptographic Puzzle Based Approach Ensuring Total Security For Transmitted Information With IP Tracing*"* *Iosr Journal Of Computer Engineering;* PP 27- 32 ep-Oct 2014.
7. Lu Han, "Wireless Ad-Hoc Networks" *Iosr Journal Of Computer Engineering* , October 8, 2004.
8. B. Mahalakshmi, S.V. Shri Bharathi, W. Lydia Shammi"Maximizing The Performance And Reliability Of Wireless Network By Preventing Jamming Attacks" *Iosr Journal Of Computer Engineering*. E- ISSN: 2278-0661, P-ISSN: 2278-8727 PP
9. 00-00; April 2010.
. .Aejaz Ahmed, H C Sateesh Kumar, "Truthful Detection Of Malicious Nodes In Ad Hoc Networks". *Ieee Transactions On Mobile Computing*
10. do:10.1109/TMC.2014
. L. Felipe Perrone, Samuel C. Nelson "A Study Of On-Off Attack Models For Wireless Ad Hoc Networks"