ASSURED NEIGHBOR BASED COUNTER PROTOCOL ON MAC-LAYER PROVIDING SECURITY IN MOBILE AD HOC NETWORKS

Gulshan Kumar and Mritunjay Rai

Department of Computer Science, Lovely Professional University, Jalandhar, India.

gulshan_acet@yahoo.com,raimritunjay@gmail.com

ABSTRACT

In this paper, we have taken out the concern of security on a Medium Access Control layer implementing Assured Neighbor based Security Protocol to provide the authentication, confidentiality and taking in consideration High speed transmission by providing security in parallel manner in both Routing and Link Layer of Mobile Ad hoc Networks. We basically divide the protocol into two different segments as the first portion concentrates, based on Routing layer information; we implement the scheme for the detection and isolation of the malicious nodes. The trust counter for each node is maintained which actively increased and decreased considering the trust value for the packet forwarding. The threshold level is defined differencing the malicious and non malicious nodes. If the value of the node in trust counter lacks below the threshold value then the node is considered as malicious. The second part focus on providing the security in the link layer, the security is provided using CTR (Counter) approach for authentication and encryption. Hence simulating the results in NS-2, we come to conclude that the proposed protocol can attain high packet delivery over various intruders while attaining low delays and overheads.

KEYWORDS

Security, Threshold level, Encryption, MAC-Layer, Attackers .

1. INTRODUCTION

1.1 Mobile Ad hoc Networks

The word Mobile Adhoc Networks (MANET) is derived from two words Mobile means moving and Ad hoc means structure less. Thus MANET refers to network comprises of nodes(devices) which are self configured and having no predefined structure thus the nodes in the network can move free. Addition and deletion of nodes from the network also have no predefined rules. Because of their self-configuration and self maintenance capabilities MANET is in marvelous attention.

1.2 Security threats

There are different types of attacks that are recorded in the current mobile adhoc networks but the most vulnerable attack on 802.11 MAC is DoS. In this form of attack the attacker may corrupt frames easily by adding some bits or ignoring the ongoing transmission. Whereas among the connecting nodes the binary exponential scheme can favour the last node which has to capture effect . In capture effect the nodes are heavily loaded and tries to consume the channel by sending

D.C. Wyld, et al. (Eds): CCSEA 2011, CS & IT 02, pp. 68–73, 2011.
 DOI: 10.5121/csit.2011.1208

the data continuously, thus resulting the lightly loaded neighbor to back off endlessly taking the factor that the malicious node will try to take the advantage of capture effect vulnerability. Whereas the nodes that tend to make the passive attack with the aim of saving battery for communication are considered to be selfish. Thus these attacks are classified as fabrication, Modification, Worm hole and Lack of Co-operation.

2. RELATED WORK

Farooq Anjoom et al. [1] gave the proposed work regarding intrusion detection in Ad hoc networks. Anand Patwardhan et al. [2] have proposed a routing protocol on AODV providing security over IPv6.

3. OBJECTIVES AND OVERVIEW OF THE PROPOSED PROTOCOL

3.1 Objectives

The motive behind this paper is to design a trust based security protocol which ensures confidentiality, Integrity and Authentication of packet in routing layer and link layer. It can also be beneficial in the application regarding high speed communication. In includes the following objectives:

- Resistance against the various attacks that include detecting evaluating and correcting the different sort of attacks
- Reliable against the energy consumption.
- Scalable in contrast to the network size
- Adjustable with amidst nodes along with the other protocol to attain high level security.
- Provides simplicity in terms of extension of network lifetime that uses basic application of ciphers like the symmetric algorithm and hash functions.

3.2 Overview of the proposed protocol

In our proposed protocol we applied certain changes on existing Ad hoc On-demand Distance Vector AODV, providing the new structure called Assured Neighbor based Counter Table (ANCT). It uses dynamical process of calculating the value of nodes in trust counter and adding the trusted nodes is prior contrasting selecting the shortest path. This protocol basically used mark and sweep process to restrict the malicious nodes to enter in the network providing the most secure network.

Let (AC_1, AC_2,…….) be the initial counter having assured nodes (N_1, N_2, …….) having the Route R_1 from Source S to Destination D. The reliability of neighbor nodes of a particular node cannot be assured initially, whether they are trusted or not and for stabilizing the route from source S to destination D, S has to send to Route Request (RREQ) packet. Forward Counter FC is used by each node to keep track of the number of packets. It has forwarded through route R. Each time, a node n_r receive a packet from node n_i, then n_r increases the Forward Counter FC of node n_i.

If

(Packet Received n_r from n_i)

Then

(Forward Counter

$FCn_i = FC_{n+1}$, where (i=1,2,3…….n) packet) ---------- (1)

After this process ANCT of node n_r is modified with node n_r is modified with the value of the forward counter $FCn_{i.}$ In the same way each node determined ANCT and finally packet reach from source S to determine D. When RREQ packet is received by the destination D, it measures the number of received packet P_R. Once the number of packet received is known, it constructs the Message Authentication Code (MAC) on P_R based on the shared key among S and D.

After this process Rote Reply (RREP) packet is created that contains the *id* of both source and destination. Based on this the MAC of P_R along with calculated route from the RREQ which will be digitally signed by the destination in RREP is send back to the source using inverse route R_1while RREP packet is reverting back from Destination D to source S, each intermediate node computes its Success Ratio (SR).

$SR_i= FCn_i/P_R$ ---------- (2)

The verification process is conducted by the intermediate node by verifying the digital signature and the MAC i.e. stored in the RREP packet. If the verification fails, the RREP packet is dropped. Otherwise further signed by the intermediate node and reverted back from destination to source in a previous manner.

If the verification process of the digital signature by the intermediate node i.e. contain in RREP is successful, then trusted counter is incremented by one, if not then decremented by one.

If successful

$TC_i=TC_i + \Delta\delta_1$

If not successful

$TCi=TCi - \Delta\delta_{1,}$

where $\Delta\delta_1$ is the step value.

Another aspect is for any node n_r, if the Success Ratio of r (SRr) is less than the minimum threshold values, then it trust counter value is decremented.

If

$SR_r<S_{min}$

Then

$TC_i =TC_i-\Delta\delta 2$, where $\Delta\delta 2$ is the step value which is less than $\Delta\delta 1$.

Now for node n_r, if the trust counter value of TC_R is less than the trusted threshold value then that node is marked as malicious. In case if the RREP is not received by the source for a time period t second, it will be consider as route is terminated or failed. Then again route discovery process is initiated by the source and same process will be repeated for R_2,R_3, etc.

1. Dynamic process of calculating the values of nodes in trust counter.
2. Adding trusted node is prior contrasting selecting the shortest path
3. Protocol use mark and sweep to restrict the malicious nodes to entire in the network which provides more secure network.

Certain changes are made on existing AODV giving a new structure called Assured Neighbors based Counter Table which maintained for each network node.

Let {Ac_1,Ac_2…….} be the initial counter having assured nodes {n_1,n_2.....} having the route R from source S to destination D. The reliability of the neighbor nodes of a particular node n cannot be assured., Initially whether they are trusted or not and for stabilizing the route from source S to destination D. S has to send the route request (RREQ) packet.

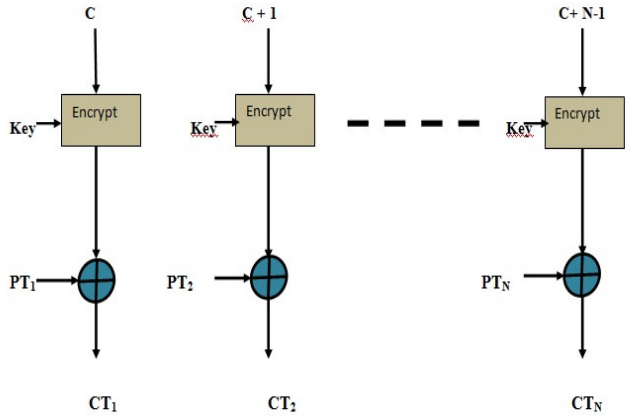


Fig: Counter Mode (Encryption)

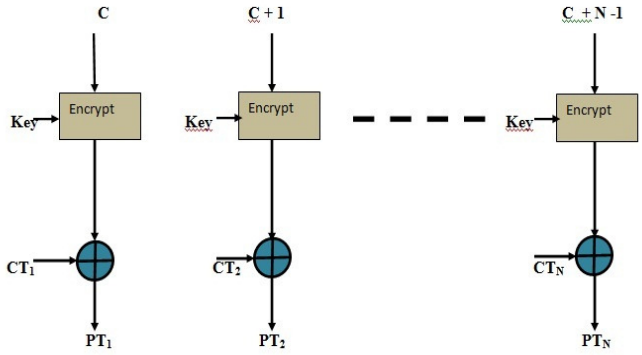


Fig: Counter Mode (Decryption)

Here, CT_i = Ciphertext [i = 1 to N] ; PT_i=Plaintext [i = 1 to N] ; C = counter value

4. PERFORMANCE EVALUATION

4.1 Simulation Model and Parameters

For the purpose of simulation we use NS2. As a MAC layer protocol we use DCF (Distributed Coordination Function) of IEEE 802.11 for wireless LANs and the channel capacity of mobile hosts are set to 2 Mbps. While simulating we have a network of 100 nodes on 1000x1000 area size. Where the radio range is 250m and simulation time is 50 sec taking Constant Bit Rate (CBR). The Packet Size is 512 bytes. Taking Random Way Point Mobility Model and varying speed to 10, 20, 30, 40, 50 m/s where Pause time is 5 m/s.

4.2 Performance Metrics

Hardware efficiency: Parallelism can be achieved by counter mode by applying this mode on multiple blocks of plaintext or cipher text.

Software efficiency: Processors that involves the features like aggressive pipelining, multiple instruction dispatch per clock cycle, number of registers and SIMD instructions can be efficiently utilized.

Preprocessing: We can see from the diagram above that the execution of the involved encryption algorithm is independent of the plaintext or cipher text. So as a preprocessing task, we can generate the output of the encryption units if proper memory and security is imposed. Next, when we shall get the plaintext or cipher text, the only thing is to be done is to calculate the XOR functions. This can enhance the efficiency of the counter mode and increase the throughput.

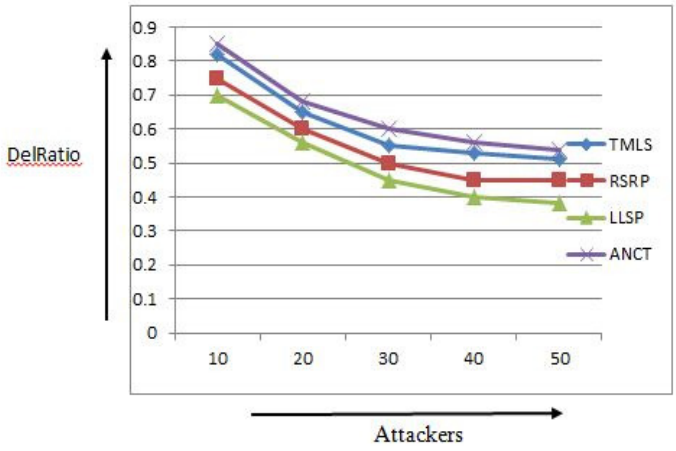
Random access: When we need to decrypt a particular block of message we need for random access. As, in this mode message blocks are independent of the processing of its previous block, random access can be easily achieved.

Provable security: As encryption is used, it must be a secure mode.

Simplicity: Here only encryption algorithm is applied and no decryption algorithm is in the view. Even, Decryption key scheduling need to be applied here.

5. RESULTS

Following is the result we evaluate on the basis of Attackers Vs Delivery ratio where our proposed protocol Assured Neighbor based Counter (ANCT) gives the best result compared to TMLS, LLSP and RSRP.



6. CONCLUSION

In our paper, we have designed Assured Neighbor based Counter Protocol which gives confidentiality, authentication and data integrity using a parallel approach of routing packets on MAC Layer in MANETs. The protocol is divided into two phases where the first phase assures the isolation and detection of malicious nodes based on routing layer information. A certain

threshold level is defined with a certain value. The trust counter for each node maintains the trust value based on which the counter value increases or decreases depending on the threshold value which decides whether the node is malicious or not. In the second phase we provide the security on the Link layer using COUNTER mode to provide authentication, integrity and encryption. By simulating our protocol we can conclude that our protocol attains high packet delivery ratio corresponding to various attackers.

REFERENCES

[1] Farooq Anjum, Dhanant Subhadrabandhu and Saswati Sarkar "Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols" in proceedings of IEEE 58th Conference on Vehicular Technology, 2003.

[2] Anand Patwardhan, Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis "Secure Routing and Intrusion Detection in Ad Hoc Networks" Third IEEE International Conference on Pervasive Computing and Communications, March 2005.

[3] S. Bouam and J. B. Othman, "Data Security in Ad Hoc Networks Using MultiPath Routing." Beijing, China: IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'03), September 2003.

[4] W. Lou, W. Liu, and Y. Fang, "SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks." Hong Kong, China: IEEE Conference on Computer Communications (INFOCOM'04), March 2004.

[5] Panagiotis Papadimitratos, and Zygmunt J. Haas, "Secure Data Communication in Mobile Ad Hoc Networks", IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2, February 2006.

[6] Ernesto Jiménez Caballero, "Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem", 2006.

[7] Yanchao Zhang, Wenjing Lou, Wei Liu, and Yuguang Fang, "A secure incentive protocol for mobile ad hoc networks", *Wireless Networks (WINET),* vol 13, No. 5, October 2007.

[8] Liu, Kejun Deng, Jing Varshney, Pramod K. Balakrishnan and Kashyap "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs", IEEE Transactions on Mobile Computing, May 2007.

Authors

Gulshan Kumar pursuing his M. Tech degree in Computer Science and Engineering from Lovely Professional University, Jalandhar, India. His research interest includes Cryptography and Mobile Adhoc Networks.

Mritunjay Kumar Rai received his Ph.D. Degree from from ABV-Indian Institute of Information Technology and Management, Gwalior, India. His research interest area is Mobile Adhoc Networks and Wireless Sensor Networks.