A TRUST BASED QUALITY OF SERVICE OF ROUTING PROTOCOL IN MANET

Chabukswar Hrishikesh

Asst. prof., CSE Dept., NBNSCOE Solapur, Maharashtra, India

Abstract - *The mobility of ad-hoc network arise security issues in network. Due to mobility of network abnormal node get easily placed in network and theft information and network is compromised. Security and providing QoS in Mobile Ad Hoc Networks (MANETs) is difficult to achieve, significantly because of the vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, the lack of a centralized monitoring or management point and the absence of a certification authority. Security is a critical issue and offers serious challenges in QoS routing in wireless ad hoc networks, and yet there is little work published in this area. Malicious attacks on MANET QoS could target many of the security properties and could be in forms of theft of service or denial of service (DoS), IP address spoofing, malicious corruption or alteration of packets, eavesdropping and etc. Group communication becomes increasingly important in MANETs because a lot of applications relay on Cooperation between a team. Video conferencing, interactive television, temporary offices and network Gaming is common examples of these applications. As a consequence, multicast routing has received significant attention over the recent years. In multicasting, a source is sending the same data to a certain set of nodes in the network. This is efficient in saving the bandwidth and improving the scalability, which is essential in MANETs.*

KEYWORDS — Authentication, Latency, Jitter, Cryptography, Integrity

1. INTRODUCTION

Ad-hoc network is a group collection of mobile node. During the last few years we have all witnessed steadily increasing growth in the deployment of wireless and mobile communication networks. Mobile ad hoc networks consist of nodes that are able to communicate through the use of wireless mediums and can form dynamic topologies. The basic characteristic of these networks is the complete lack of any kind of infrastructure, and therefore the absence of dedicated nodes that provide network management operations as do the traditional routers in fixed networks. In order to maintain connectivity in a mobile ad hoc network all participating nodes have to perform routing of network traffic. The cooperation of nodes cannot be enforced by a centralized administration authority since that does not exist. Therefore, a network-layer protocol designed for such self-organized networks must enforce connectivity and security requirements in order to guarantee the undisrupted operation of the higher layer protocols. Unfortunately all of the widely used ad hoc routing protocols have no security considerations and trust all the participants to correctly forward routing and data traffic. Figure (1) shows that mobile ad-hoc network scenario

Figure 1: shows that scenario of ad-hoc network

Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. There is no fixed infrastructure such as base stations for mobile switching. Nodes within each other's radio range communicate directly via wireless links while those which are far apart rely on other nodes to relay messages. Node mobility causes frequent changes in topology. The wireless nature of communication and lack of any security infrastructure raises several security problems .The nature of ad hoc networks poses a great challenge to system security designer's due to the following reasons: firstly, the wireless network is more susceptible to attacks ranging from passive eavesdropping to active interfering; secondly, the lack of an online CA or Trusted Third Party adds the difficulty to deploy security mechanisms; thirdly, mobile devices tend to have limited power consumption and computation capabilities which makes it more vulnerable to Denial of Service attacks and incapable to execute computation-heavy algorithms like public key algorithms; fourthly, in MANETs, there are more probabilities for trusted node being compromised and then being used by adversary to launch attacks on networks, in another word, we need to consider both insider attacks and outsider attacks in mobile ad hoc networks, in which insider attacks are more difficult to deal with; finally, node mobility enforces frequent networking reconfiguration which creates more chances for attacks, for example, it is difficult to distinguish between stale routing information and faked routing information. There are five main security services for MANETs: authentication, confidentiality, integrity, non-repudiation, availability.

2. PROPOSED ALGORITHM

In this paper we proposed a cryptography approach for prevention of network by malicious attack and improve the quality of service in ad-hoc network. Review study gives outlines of related work to cryptography approach for prevention and detection of malicious attack. Here process of cryptography uses cyclic-shift approach.

Cyclic Shift and Bit wise Exclusive OR (XOR)

Let, x is a block of n-bits. A cyclic shift to the left by m bits is performed by taking the first m bits from the left side of the block and attaching them to the right side. Accordingly, a cyclic shift to the right by m bits is performed by taking the first m bits from the right side and attaching them to the left side. Table 1 shows the multiplication of '03' and it is followed by Table 1 which shows that by using cyclic shift operation, then XOR by the number itself, it will produce the same result as Table4.1.

D	H	Binary (A)	'03' (C)	Y=A x C	Hex
1	1	00000001	11	00000011	03
2	2	00000010	11	00000110	06
3	3	00000011	11	00000101	05
4	4	00000100	11	00001100	0C
5	5	00000101	11	00001111	0F
6	6	00000110	11	00001010	0A
7	7	00000111	11	00001001	09
8	8	00001000	11	00011000	18
9	9	00001001	11	00011011	1B
10	A	00001010	11	00011110	1E
11	B	00001011	11	00011101	1D
12	C	00001100	11	00010100	14
13	D	00001101	11	00010111	17
14	E	00001110	11	00010010	12
15	F	00001111	11	00010001	11

TABLE 1: Finite Field multiplication of '03' in binary and hexadecimal

So that for '0E','0D','0B' and '09' finite field multiplication:

'0E' = (((A<<1) XOR A) <<1) XOR A) << 1

'0D' = ((A<<1) XOR A) <<2) XOR A

'0B' = (A<<1) XOR A) XOR (A<<3)

'09' = ((A << 3) XOR A)

It was found that in new approach technique, GF (2^8) multiplications, which is the best method that can be

implemented by table look-up has been replaced by cyclic shift and XOR operation. A session key is a single-use symmetric key used for encrypting all messages in one communication session. A closely related term is content encryption key (CEK), traffic encryption key (TEK), or multicast key which refers to any key used to encrypt messages, as opposed to other uses, like encrypting other keys (key encryption key (KEK) or key wrapping key). Session keys can introduce complication into a system, normally to an undesirable end also help with some real problems. There are two primary reasons to use session keys:

- First, several cryptanalytic attacks become easier as more material encrypted with a specific key is available. By limiting the amount of data processed using a particular key, those attacks are made more difficult.
- Second, asymmetric encryption is too slow for many purposes, and all secret key algorithms require that the key is securely distributed. By using an asymmetric algorithm to encrypt the secret key for another, faster, symmetric algorithm, it's possible to improve overall performance considerably. This is the process used by PGP and GPG.

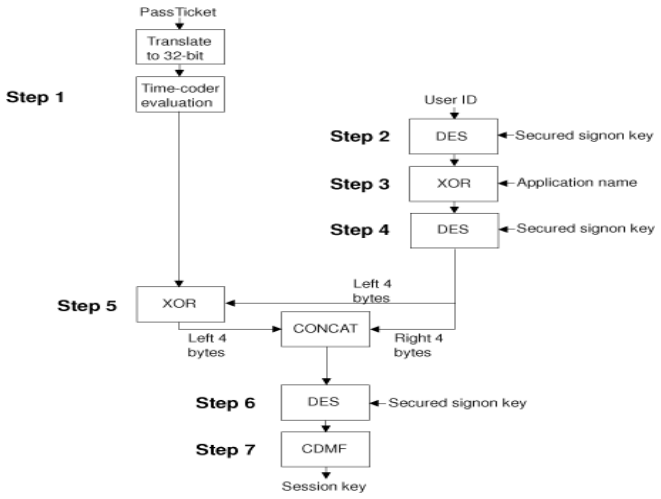

Figure 2: shows that steps of session key generation

Now we have proposed a new methodology for generate of id key for the authentication of node this method based on Cycle chain shift mechanism. In this mechanism the previous record of data are automatic destroy .That means the process of key generation maintain a process for independency of next value. Here we used some convention notation for our algorithm:-

(1) {N1,IN.N2} The set of notation represent the value of sources node, intermediate node and destination node.
(2) Sk = Session key.
(3) (Ki)s = secrete key.
(4) Cid = the communication and its identity.
(5) VT = represent value of communication, it equals h{V1,V2,V3}
(6) Token = generated token
(7) (X) =message.
(8) h(X) = hashed message

Here discuss the dynamic key generate which is the main contribution in our proposed in addition to the type of confidential information shared between the two node. Our scheme require two set of keys to be generated at each party's side: secondary keys (Ki)s and session key (SK)s . (Ki)s are necessary to generate V values ,which are used as a security enhancement step to generate session keys. The node N1 will issue the intermediate node (IN) and a communication authentication once authenticated.

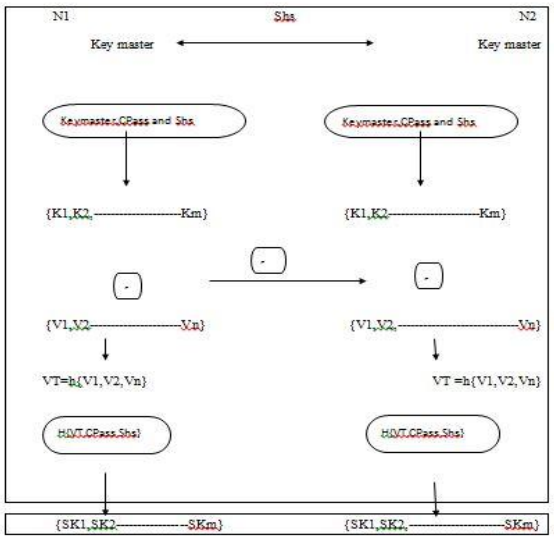

Figure 3: shows proposed key generation technique for MANET

The generation of (Ki)s is relies on the combination of three mentioned factors, Keymaster, CPass and Shs as follows :-

Ki = h{Keymaster,CPass,Shs}

Ki+1 = h{CPass,Shs,Ki}

Ki+2 = h{Shs,Ki.Ki+1}

Ki+3 = h{Ki,Ki+1,Ki+2}

Km = h{Km-3,Km-2,Km-1}

The first generation (Ki) relies on at least existence of three factors, whereas the next generation keys eliminate one of them after each generation step. The same shifting technique is applied for SKs generation as well. After the generation of (Ki)s, N1 and IN start generating V values (V1,V2,V3)as follows:

V1 = r mod(m-3)

V2 = r mod(m-2)

V3 = r mod(m-1)

Where m-3,m-2 and m-1 are hashed values of the last calculated secondary key (Ki). The generated V values will then be hashed to generate VT value, Which is one of the pillars in generating (SK)s as follows:

VT = h{V1,V2,V3}

We will then use VT,CPass and Shs to generate (SK)s as shown below :

SK1 = h{VT,CPass,Shs}

SK2 = h{CPass,Shs,SK1}

SK2 = h{CPass,SK1,SK2}

SK3 = h{SK1,SK2,SK3}

SKm = h{SKm-3,SKm-2,SKm-1}

The main concept is to apply one hash algorithm with cyclic shifting of master secret each time a session key is generated.

Outcomes

- Reduce the traffic overhead
- Better detection of wormhole and malicious node detection in mobile ad-hoc network.
- Reduce the delay rate of node communication.

3. CONCLUSIONS

The aim of this paper is to propose an effective and efficient scheme which promises packet dropping on the time of node authentication based on cryptography approach for improvement of quality of service. This scheme covers the following activities simultaneously, Provide node authentication in ad-hoc network, Reduces packet dropping. Remove node ambiguity.

REFERENCES

[1]ShahrzadSedaghat, FazlollahAdibniya and ValiDerhami" A Secure Mechanism for QoS Routing in Mobile Ad Hoc Networks with QoS Requirements Consideration" in International Conference on Computational Intelligence and Communication Networks in 2010.

[2] Mohammad M. Qabajeh , Aisha H. Abdalla, Othman Khalifa and Liana K. Qabajeh" A Tree-based QoS Multicast Routing Protocol for MANETs" in International Conference on Mechatronics (ICOM), in 2011.

[3] Ming Yu, and Kin K. Leung, Fellow" A Trustworthiness-Based QoS Routing Protocol for Wireless Ad Hoc Networks" in IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 4, APRIL 2009.

[4] Kirk Chang, Gitae Kim, Larry Wong and Sunil Samtani "network layer congestion control to ensure quality of service (qos) in secure battlefield mobile ad hoc networks" in IEEE Transaction 2010.

[5]G. Santhi, Dr. Alamelu Nachiappan and MougamadouZaidIbrahime[p6] "Q-learning based adaptive QoS routing protocol for MANETs" in IEEE-ICRTIT 2011.

[6] Y. Zhou and Y. Fang, "Scalable and deterministic key agreement for large scale networks," IEEE Trans. Wireless Commun., vol. 6, no. 12, pp. 4366-4373, Dec. 2007.

[7] W. Liu, W. Lou, and Y. Fang, "An efficient quality of service routing algorithm for delay-sensitive applications," Computer Networks, vol. 47, no. 1, pp. 87-104, 2005.

[8] P. P. C. Lee, V. Misra, D. Rubenstein, "Distributed algorithms for secure multipath routing in attack-resistant networks," IEEE/ACM Trans. Networking, vol. 15, no. 6, pp. 1490-1501, Dec. 2007.

BIOGRAPHIES

Chabukswar Hrishikesh, Asst. prof., CSE Dept., NBNSCOE Solapur, Maharashtra, India

