Identity Based Cryptography for Secure AODV Routing Protocol

Ali M. Sagheer, *IEEE Member,* and Hadeel M. Taher

***Abstract* — Mobile Ad hoc Network (MANET) is crowd of mobile node communicates and participate in network operation unused to fixed base station each node depended on the other node to deliver the packet that send from source node to destination. Ad hoc network needed secure routing protocols to protect network from many threat in its environment, In this paper we used Identity Based Cryptography (IBC) that have many advantage compared to traditional cryptosystems for Secure AODV (Ad hoc On demand Distance Vector routing) routing protocol.**

***Keywords* — MANET, Secure Routing, AODV Protocol, Identity Based Cryptography.**

I. Introduction

Ad Hoc means in Latin "formed for" or "concerned with one specific purpose", nodes in Ad Hoc Networks are freedom to move, they may act as both host and router, and each node can be trust traffic on anther nodes maintaining connectivity in a decentralized manner. That's why Ad hoc Network is also known as infrastructureless network, also nodes are self-forming and self-configuring.[1], [2]. It has many characteristic that differentiate it from other wireless network include: Dynamic deployment, Wireless medium less dependable than wired medium, Limited Capacity and Bandwidth, Energy life in mobile node power resources can be replaced by users, and the Security because mobile nodes in the network its prone to many kind of attacks [3]. Routing protocols for Mobile Ad Hoc Networks is very important to ensure deliver packet to appropriate distantion it can be classified to: (i) Table Driven or Proactive Protocols is updated every time the topology changes [4]. (ii) On Demand or Reactive Protocols is obtaining to create a path to a destination only when node in the network demands for it [5]. (iii) Hybrid Routing Protocols in this type is mixed between the above types [4]. Although all these routing protocols for Mobile Ad Hoc Networks without any protect from any type of attack. We used Cryptography for improve security to AODV protocol. Cryptography is an operative method of defensive sensitive information as it is kept on media or transmitted through network communication routes. The main reason for use cryptography for hide information from anyone unauthorized those called attackers, if the attacker has enough time, desire, and resources the algorithms can be destroyed and the information can be exposed [6]. Cryptography can classified into two type: secret key is also known as symmetric cryptography is single key used for both encryption and decryption but the major difficulty with this method is the distribution of the key that it's solved by the another type is public key (asymmetric) cryptograph public cryptography [7].

The uniformly distributed keys in encryption and decryption it's the same between communication parties the authentication can only be achieved for that reason public-key cryptography is used to solve the problem of key agreement or distribution, this render public key more suitable for MANETs. Nonetheless the Traditional public key cryptography usually used when dependence on a Public Key Infrastructure (PKI), that means it has a Certificate Authority as principal control point that every node in MANET must be trusted in this point. That is a big obstacle with the MANET characteristics also this PKIs make MANETs is more overhead in storage and packet transmission. So that for all those reasons the special method of asymmetric cryptography known as Identity-based cryptography (IBC) is a more suitable solution to increase security in MANET [8], [9].

II. Related Work

MANETs was derivation through the military, define by the Defense Advanced Research Projects Agency (DARPA) that supported packet radio (PRNET) networks in 1970s, then still developing until Ad Hoc Networks entered a new stage of growth due to the popularity and the idea of an infrastructure less crew of mobile hosts was proposed, and its stall to develop. Cryptography is used to provide security goals for Ad Hoc Network because increase threats in network [8], [10]. Shamir was first proposed the idea of Identity-based cryptography, he proposed it can be enables any pair of nodes to communicate securely and to verify each other's signatures without exchanging private or public keys, by calculate public key through chooses his name and network address, while secret key is computed by Private Key Generator which can be privileged situation by knowing some secret information that enable it to calculate the secret keys of all users in the network. After Shamir announced his idea not developed quickly [11]. Boneh and

Ali Makki Sagheer is with the College of Computer, University of Anbar, Ramadi, Anbar,Iraq (phone: 00964-770-0073940; e-mail: ali_makki@ieee.org).

Hadeel M. Taher is with the College of Computer, University of Anbar, Ramadi, Anbar,Iraq (phone: 00964-781-6729696; e-mail: hadelmtf@yahoo.com).

978-1-4673-2984-2/12/$31.00 ©2012 IEEE

Franklin in 2001 proposed Identity-Based Encryption from the Weil Pairing. They offer a completely practical Identity-Based Encryption scheme (IBE) and provide accurate definitions for secure identity based encryption schemes [12]. Adjih et al in 2005, propose secure OLSR using IBC. Their suggestion TA is in charge of certifying or assigning keys of each node joining in the trusted network. Each node sharing the network will have the public key of the TA as global key; any node entering the ad hoc network could deployment its public keys, with a specific key exchange protocol, with proper parameters and signatures. Key that used later to sign message is called the local key. A node would start creating OLSR control messages, signing them using the local key with a specific addition which prepends a special signature message [1], [8].

III. Secure Routing Approaches In Mobile Ad Hoc Networks

The Routing protocols were presented for ad hoc networks deal with changing deployment of mobility nodes. Secure Routing protect against any threat on the network [5]. The information that transmitted between mobility nodes must be route by routing protocols this information is the aim of many threats. There are two threat types on secure routing [10]. One came from outside the network called external by inserting, replaying, or distorting information. Another threat came from inside network by compromised nodes, which may it announce false information to other nodes to distinguish this information is very difficult because vulnerable nodes are capable to create legal signatures using their private keys [13]. For protected from the first threat by using cryptographic schemes for ensure security routing information, this way is not effective for the second threat. But it not necessity to ignore this type ,the detection of compromised nodes through routing information difficult in an ad hoc network as a result of changing deployment [2]. The routing protocol should be capable to discovery paths that go around these vulnerable nodes. Routing protocols can discover multiple directions for example protocols in DSR , AODV and ZRP , nodes that use these protocol can change to an another route when the main route appears to have unsuccessful [4].

IV. The Proposed Secure AODV Routing Protocol via IBC Algorithm

We propose a Secure AODV (SAODV) routing by using ID based cryptography because in which In Mobile Ad Hoc Network various approaches used cryptographic to enhancement security for routing protocol for instance in SAODV used digital-signature based scheme for protected AODV from vulnerable or compromise by any kind of threat can make broadcast message authentication, but they needed to the certificate that suffered from large amount overhead in communication and storage. And Secure Routing Protocol used Hashed Message Authentication Code based schemes, HMAC provide authentication to the message between only two nodes connect and cannot broadcast message authentication for that reason they are not appropriate for broadcasting-based routing messages and also required to certificate, While hash-chain-based such as Ariadne and identity based secure routing, this based on use the time synchronization but it may not be achievable intended for common uses. By another mean before secure communications can occur, both source node and destination node requirement to generate encryption and signature key pairs, demand from certificate with evidence of identity to a Certificate Authority (CA), then after receive signed certificates that use to authenticate one another and give-and-take encrypted data. This procedure can be both time-consuming and error-prone. But to solve a lot of these problems it must be use the IBC for special properties enabling effective authentication in MANETs. IBC are unlike conventional public key infrastructure schemes, IBC not generate any storage overhead and communication overhead for storing and is very useful for a deployment in MANETs.

A. IBC Settings

The principal method of identity-based cryptography generates the master key and public parameter by the Private Key Generator Center (PKG). However, the form the IBE system uses the Weil pairing on elliptic curves. The definition of is denoted: $\hat{e} : G1 \times G1 \rightarrow G2$. Let G1, G2 be group of an elliptic curve with order q (q is a prime), agreeable the next conditions:

- Bilinear: $\hat{e}(aP, bQ) = \hat{e}(P,Q)^{ab}$ for all $P,Q \in G1$ and all $a, b \in Z^{*}q$. This can be also show in another way : For $P,Q,R \in G1$, $\hat{e}(P + Q,R) = \hat{e}(P,R)\hat{e}(Q,R)$ and $\hat{e}(P,Q + R) = \hat{e}(P,Q)\hat{e}(P,R)$.
- Non-degenerate: P is a generator for G1, then $\hat{e}(P,P) \neq 1$.

Computability: Set $P,Q \in G1$, there is $\hat{e}(P,Q)$ be computable.

B. IBC Algorithm

An identity scheme is identified by four randomized algorithms: Setup, Extract, Encrypt, and Decrypt.

- *Set-up:* This algorithm takes as input a security parameter k and returns the system parameters PP together with the master secret key msk. The system parameter must include the description of the message space $\mathcal{M}$, the cipher text $\mathcal{C}$, the identity space $\mathcal{I}$ and the master public key. They are publicly known while the master secret key is known only to Private Key Generator (PKG).
- *Key-Generation*: This algorithm takes as input a parameters PP together with identity $id \in I$ and master secret key msk and outputs private key did using the master key. The identity id is used as public key while did is its corresponding private

key.

- *Encryption*: This algorithm takes as input an identity $id \in I$, system parameters *PP* and message M and produces the output a ciphertext $C \in \mathcal{C}$.
- *Decryption:* This takes as input system parameters *PP*, a ciphertext $C \in \mathcal{C}$, an identity *id* and corresponding private key *did* and returns the corresponding plaintext.

C. Securing AODV Routing Process

AODV secure by ID based cryptography protocol is on-demand protocol characteristics and discovers routes when require through a route discovery process. Its uses Secure Route Request (SRREQ), Route Reply (SRREP) control messages in Route Discovery process and Route Error (RERR) control message in Route Maintenance process. When a source node is concerned to communicate with a destination node, it broadcasts a SRREQ route request packet that contains node IP addresses, a Request ID (Public key of node), source and the destination, sequence numbers along with a hop count is set to zero and flags and a signs the packet with its private key. When the secure request packet reached to intermediate node first verifies the signature of the source node in the SRREQ for insure if this packet sent to this node or not, when the signature is verified then know this is the target node and setting up to sending SRREP but if the signature is not verified then the SRREQ is dropped. When the secure request packet reached to the destination node, then they generate a reply route packet called a SRREP and sent it to the source node. SRREP packet include route epoch time, a hop count, the destination node sequence number, the source and the destination IP addresses, and flags. When nodes take delivery of secure reply packet, increases the hop count, and transform secure reply packet in opposite route for reached to source node. In this protocol it uses HELLO messages from time to time to find connection failures to nodes that it considers as its neighbors node. What time a connection failure is discovered for a next hop of the route a RERR route error message is sent to its dynamic neighbor's nodes use via the individual route.

V. Implementation

The simulation software that used in this paper called Network Simulator (NS). NS is discrete-event driven simulation software designed for network simulation; the simulator tool used is NS-2 (version 2.35) installed in a LINUX (Ubuntu 10.11) to avoid this disadvantage by install it on windows. The above described secure AODV scheme was combined into the existing AODV code in the NS-2, with the persistence of securing the routing packets; this wants several modifications to be prepared to the existing NS-2 AODV implementation. Simulation parameters of the scenarios of secure AODV have been determined for instance TCL parameters in NS-2, which are brief in "Table 1". We have practical CBR sources (for traffic model) that started at any times to acquire a common view of exactly how routing protocols behave.

Table 1: Simulation Parameters.

Parameter	*Value*
Network Simulator	NS-2 2.35
Channel type	Wireless channel
MAC protocol	IEEE 802.11
Network interface model	Phy/WirelessPhy
Data (traffic) type	CBR
Antenna model	Omni Antenna
Simulation area	670*670
Number of nodes	20
Data packet size	512
Propagation model	Two ray Ground
Routing protocol	AODV
Queue type	PriQueue
Network interface queue	DropTail/priQueue
Node placement	random

VI. Experimental Results And Discussion

In the final the discussion approximately for the above explained to give the person who reads a brief understanding of the performance of the proposed of the secure routing protocol in mobile ad hoc network based on ID based cryptography. For example, in this paper, we take the number of nodes equivalent 20 moving over an area randomly. The results from NS-2 (version 2.35) simulation environment show better performance of security of AODV based on ID based cryptography is better than AODV. There are three parameter used to show the difference between the secure AODV using ID based cryptography and the original AODV these are: Throughput of sending packets, Throughput of receiving packets, Sum of number of all packets dropped.

VII. Conclusion

In the previous sections, the proposed secure routing protocol for MANET was presented, and the effect of its parameters on enactment, such as the number of sending packets, Throughput of receiving packets, Sum of number of all packets dropped. The ID based cryptography scheme has been implemented and the same is integrated into the AODV. This proposed to secure routing protocol from any node being malicious by increased the capability to secure itself from any unauthorized nodes, another important thing is the time that required in signature generation and verification, finally Aho, Peter Weinberger, and Brian Kernighan (AWK) tool used to be very advantageous to use in analyses of the a lot of end result from NS-2 for determining changed performance evaluation metrics in future work we can Applying the proposed secure routing protocol AODV on other simulators such as the other network simulation tools contain OPNET [OPNET], Glomosim [GLO], Qualnet [QUAL] and OMNET++ [OMN], for guarantee secure AODV enchantment.

REFERENCES

[1] Ç. Erdal and R. Chunming, Security in Wireless Ad Hoc and Sensor Networks, 1st ed , A John Wiley and Sons, Ltd, Publication, United Kingdom, 2009.

[2] T. Sunil and K. Ashwani,"A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010.

[3] S. Kuldeep, K. Neha and M. Prabhakar, " An Overview Of security Problems in MANET", [Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02, 2010.

[4] P. Niroj, "A secure Zone-based routing protocol For Mobile ad hoc networks", M.S. thesis, Dep. Computer Scie., Department of Computer Science and Engineering National Institute of Technology, India May 2009.

[5] S. Kimaya, L. Brian, S. Clay, D. Bridget, R. Elizabeth, "A Secure Routing Protocol for Ad Hoc Networks", IEEE 10 th, International Conference on Network Protocols,2002.

[6] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, Vol 1, No. 15, Haryana, 2010. K. Anil and R. Sanjeev, "Identity-Based Key Management in MANETs using Public Key Cryptography", International Journal of Security, Vol 3, India.

[7] S. Zhao, A. Aggarwal, R. Frost and X. Bai, "A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks", IEEE Communications Surveys & Tutorials, 1553-877X/11/$25.00, 2011.

[8] J. Marc and N. Gregory, Identity-Based Cryptography, IOS Press, ISBN 978-1-58603-947-9, 2009.

[9] S. Deepak, S. Saxena, S.Yogesh and T.Ajay, "Identity Based Secure Routing For Wireless Ad-Hoc Networks", International Journal of Recent Trends in Engineering, Vol 2, No. 1, November 2009.

[10] Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, 1979.

[11] Boneh and Franklin, "Identity-based encryption from the weil pairing," in Proc. Crypto 2001, ser. LNCS, vol. 2139. Springer, 2001.

[12] N. Pushpendra, S. Prashant, S. Raj kumar and P. Ram, " Detection of Wormhole Attack using Hop-count and Time delay Analysis", International Journal of Scientific, Vol 2, Issue 4, India, April 2012.

[13] J. Rutvij, P. Ashish, P. Jatin and S. Bhavin , "MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.