www.ijiarec.com

ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Effective Pre-Secure Communication Data Sharing Model for MANET using GECC Algorithm

[1]Mr. R. NavinKumar M.C.A., M.Phil., Assistant Professor,
[2]Mr.R.Sudhakar Final MCA .,
Department of MCA , Nandha Engineering College (Autonomous), Erode-52.
E-Mail ID: navinsoccer07@gmail.com, sudhakarrajendran97@gmail.com

***Abstract*- Mobile autonomous networked systems have seen increased usage by the military and commercial sectors for tasks deemed too monotonous or hazardous for humans. MANET communication is commonly wireless. Wireless communication can be trivially intercepted by any node in range of the transmitter. This can leave MANETs open to a range of attacks, such as the Sybil attack and route manipulation attacks that can compromise the integrity of the network.Autonomous systems require a significant amount of communication. Problem solving techniques, such as distributed task allocation are required to solve task planning problems without human intervention and these techniques are vulnerable to packet loss and false messages; partial data will lead to sub-optimal or failed task assignments.To protect these networks, security protocols have been developed to protect routing and application data. To address these problems, a classic secure framework is proposed. The framework is designed to allow existing network and routing protocols to perform their functions, even as providing node authentication, access control, and communication security mechanisms.The Security Using Pre-Existing Routing for Mobile Ad-hoc Networks (SUPERMAN). The protocol is designed to address node authentication, network access control and secure communication for MANETs at the network layer**

***Keywords*— MANET,WSNs,SAMAC,MES**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed Algorithms, programming models, data management, security and social factors. Wireless sensor network applications include ocean and wildlife monitoring, manufacturing machinery performance monitoring, building safety and earthquake monitoring, and many military applications.

An even wider spectrum of future applications is likely to follow, including the monitoring of highway traffic, pollution, wildfires, building security, water quality, and even people's heart rates. A major benefit of these systems is that they perform in-network processing to reduce large streams of raw data into useful aggregated information. Because sensor networks pose unique challenges, traditional security techniques used in traditional Networks cannot be applied directly.

II.RELATED WORKS

David Pointcheval and Jacques Stern

Since the appearance of public-key cryptography in the seminal Diffie-Hellman paper, many new schemes have been proposed and many have been broken. Thus, the simple fact that a cryptographic algorithm withstands cryptanalytic attacks for several years is often considered as a kind of validation procedure. A much more convincing line of research has tried to provide provable security for cryptographic protocols. Unfortunately, in many cases, provable security is at the cost of a consider-able loss in terms of efficiency. Another way to achieve some kind of provable security is to identify concrete cryptographic objects such as hash functions with ideal random objects and to use arguments from relative complexity theory.

The model underlying this approach is often called the random oracle model. They use the word arguments for security results proved in this model. As usual, these arguments are relative to well-established hard algorithmic problems such as factorization they offer security arguments for a large class of known signature schemes. Moreover, they give for the first time an argument for a very slight variation of the well-known ElGamal signature scheme. Inspiteof the existential forgery of the original scheme, they proved that our variant resists existential forgeries even against an adaptively chosen-message attack. This is provided that the discrete logarithm problem is hard to solve.
Michael K. Reiter, Aviel D. Rubin

In this paper we introduce a system called Crowds for protecting users' anonymity on the world-wide-web. Crowds, named for the notion of blending into a crowd", operates by grouping users into a large and geographically diverse group (crowd) that collectively issues requests on behalf of its members. Web servers are unable to learn the true source of a request because it is equally likely to have originated from any member of the crowd, and even collaborating crowd members cannot distinguish the

originator of a request from a member who is merely forwarding the request on behalf of another. We describe the design, implementation, security, performance, and scalability of our system. Our security analysis introduces degrees of anonymity as an important tool for describing and proving anonymity properties. The lack of privacy for transactions on the world-wide-web, or the Internet in general, is a well-documented fact. While encrypting communication to and from web servers can hide the content of the transaction from an eavesdropper (e.g., an Internet service provider, or a local system administrator), the eavesdropper can still learn the IP addresses of the client and server computers, the length of the data being exchanged, and the time and frequency of exchanges. Encryption also does little to protect the privacy of the client from the server. A web server can record the Internet addresses at which its clients reside, the servers that referred the clients to it, and the times and frequencies of accesses by its clients.
David Chaum

Keeping confidential who sends which messages, in a world where any physical transmission can be traced to its origin, seems impossible. The solution presented here is unconditionally or cryptographically secure, depending on whether it is based on one-time-use keys or on public keys, respectively. It can be adapted to address efficiently a wide variety of practical considerations. Three cryptographers are sitting down to dinner at their favorite three-star restaurant. Their waiter informs them that arrangements have been made with the maitre d'hotel for the bill to be paid anonymously. One of the cryptographers might be paying for the dinner, or it might have been NSA (U.S. National Security Agency). The three cryptographers respect each other's right to make an anonymous payment, but they wonder if NSA is paying. They resolve their uncertainty fairly by carrying out the following protocol: Each cryptographer flips an unbiased coin behind his menu, between him and the cryptographer on his right, so that only the two of them can see the outcome.

In case the two coins he sees are the same, one of the other cryptographers said "different," and the other one said "same." If the hidden outcome was the same as the two outcomes he sees, the cryptographer who said "different" is the payer; if the outcome was different, the one who said same is the payer. David L. Chaum

Another use allows an individual to correspond with a record-keeping organization under a unique pseudonym which appears in a roster of acceptable clients.
David Pointcheval and Jacques Stern

In this paper, authors address the question of providing security proofs for sig-nature schemes in the so-called random oracle model In particular, we establish the generality of this technique against adaptively chosen message attacks. Our main application achieves such a security proof for a slight variant of the ElGamal signature scheme where committed values are hashed together with the message. This is a rather surprising result since the original ElGamal is, as RSA , subject to existential forgery.

Since the appearance of the public key cryptography, in the famous Diffie-Hellman paper, a significant line of research has tried to provide provable security for cryptographic protocols. In the area of computational security, proofs have been given in the asymptotic framework of complexity theory. Still, these are not absolute proofs since cryptography ultimately relies on the existence of one-way functions and the P vs. N P question. Rather, they are computational reductions to and from well established problems from number theory such as factoring, the discrete logarithm problem or the root extraction problem, on which RSA relies . In the present paper they will exclusively focus on signatures. As shown in the Diffie-Hellman paper , the trapdoor function paradigm allows creating signatures in the public key setting. Nevertheless, both the RSA scheme and the ElGamal scheme are not provably secure since they are subject to existential forgery.

III. METHODOLOGY

SUPERMAN provides security to all data communicated over a MANET. It specifically targets the attributes of MANETs; it is not suitable for use in other types of network at this time. It sacrifices adaptability to a range of networks, to ensure that MANET communication is protected completely and efficiently. A single efficient method protects routing and application data, ensuring that the MANET provides reliable, confidential and trustworthy communication to all legitimate nodes.

The proposed work includes the implementation of SUPERMAN on a simple mobile node platform to allow experimental observation and profiling of its performance, the proposal of network bridging solutions capable of providing SUPERMAN services between two closed networks over an insecure intermediate network, and investigating the effects of variable network topology on SUPERMAN to better understand the role of the credential referral mechanism on overhead mitigation in SUPERMAN networks.

PROPOSED MODEL

The proposed system develops a source anonymous message authentication code (SAMAC) on elliptic curves that can provide unconditional source anonymity. It offers an efficient hop-by-hop message authentication mechanism for MANETs without the threshold limitation. It devises network implementation criteria on source node privacy protection in MANETs. It proposes an efficient key management framework to ensure isolation of the compromised nodes.

Propose an unconditionally secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified ElGamal signature (MES) scheme on elliptic curves. This MES scheme is secure against adaptive chosen-message attacks in the random oracle model. Our scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the mobile node power. While achieving compromise- resiliency, flexible-time authentication and source identity protection, our scheme

does not have the threshold problem.

1. SYSTEM CONFIGURATION

Trusted Authority (TA)

- A static node responsible for node initialisation and provision of certificates; it is a prerequisite to SUPERMAN.
- Certificate (CKp) o Required per node and shared with other nodes to join the network
- Public Diffie-Hellman Key Share (DKSp) o A public value communicated between nodes
- Private Diffie-Hellman Key Share (DKSpriv)
- A private value, held by all nodes in the network and never communicated. Used as the shared secret for Diffie-Hellman key exchange
-

2. NETWORK CONSTRUCTION

In this module, 'n' number of nodes is created with hop distance from base station node. The details are saved in 'WSN' table. In this module, Wireless Sensor Network is displayed graphically like the one in the network.

3. SECURE NODE-TO-NODE KEYS

In this module SKe keys are used to secure end-to-end communication with other nodes, with one SKe key generated per node, for every other node also authenticated with the network. SKp keys are used for point-to-point security and generated in the same manner as SKe keys**.**

4. SECURE POINT-TO-POINT FOOTERS

In this module secure footers is to all node communication packets sent between SUPERMAN nodes. *SKbp* and *SKp(x)* keys are used in broadcast and unicast integrity service provision respectively.

5. END-TO-END COMMUNICATION

End-to-end security provides security services between source and destination nodes by using their shared SKe. Confidentiality and integrity are provided using an appropriate cryptographic algorithm, which is used to generate an encrypted payload (EP).

6. MESSAGE GENERATION IN SOURCE NODE

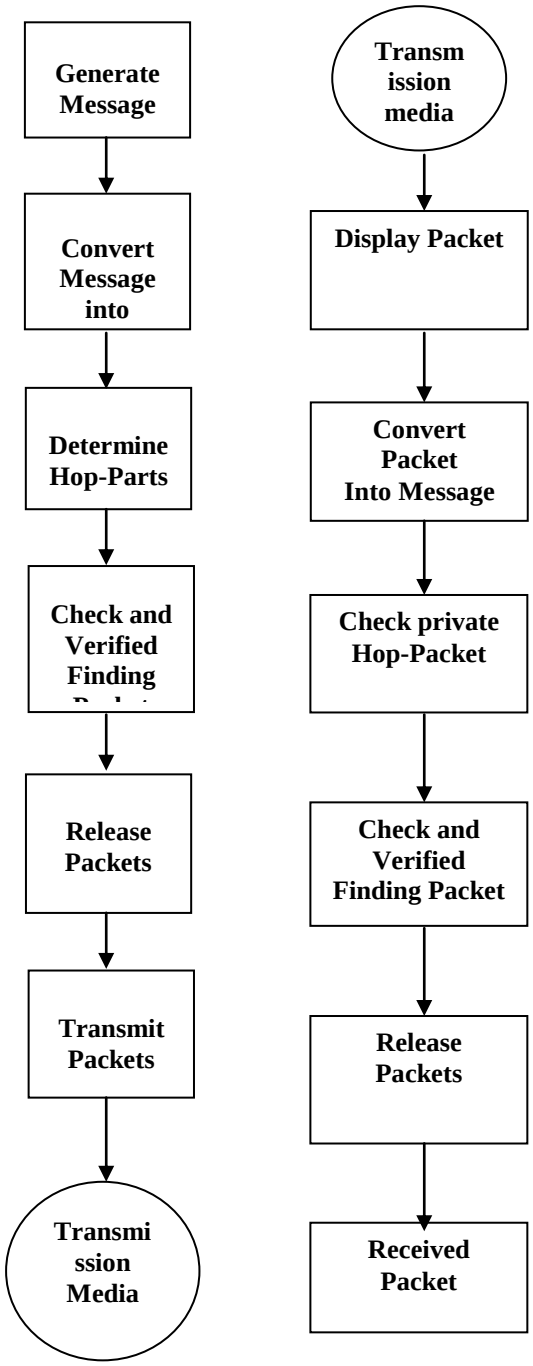
In this module, the message is generated in source node. The message receiver should be able to verify whether a received message is sent by the node that is claimed, or by a node in a particular group.

Hop-by-hop message authentication: Every forwarder on the routing path should be able to verify the authenticity and integrity of the messages upon reception.

Identity and location privacy: The adversaries cannot determine the message sender's ID and location by analyzing the message contents or the local traffic.

7. MESSAGE VERIFICATION IN SINK NODE OR BASE STATION

Verification algorithm: In fact, if the scheme has been correctly generated without being modified, then we compute



SYSTEM ARCHITECTURE

In hop by hop message transaction, first a message has been generated. The generated message is converted into the packets, and then by the performance of the hop, the packets are determined to choose the hop parts. The packets are processed into the hop by checking and verifying the public key using elliptical curve cryptography in the node and transmit the packet to the transmission media; the process are represented in Fig 3.4.1.

The transmission media receives and display the packet and the packet is converted into the message by checking and verifying the key with the help of geometrically elliptical curve cryptography method. Finally the released packet is received with the corresponding packet.

MESSAGE GENERATION IN SOURCE NODE

In this section, the message is generated in source node. The message receiver should be able to verify whether a received message is sent by the node that is claimed or by a node in a particular group.

Hop-by-hop message authentication: Every forwarder on the routing path should be able to verify the authenticity and integrity of the messages upon reception.

Identity and location privacy: The adversaries cannot determine the message sender's ID and location by analyzing the message contents or the local traffic.
Message is generated like the following:

Generate (m, Q1, Q2,..., Qn). Given a message m and the public keys Q1, Q2,..., Qn of the AS (Ambiguous Set) S={A1,A2, ... ,An}, the actual message sender At, 1 <= t <= n, produces an anonymous message S(m) using its own private key dt. Verify S(m). Given a message m and an anonymous message S (m), which includes the public keys of all members in the AS, a verifier can determine whether S (m) is generated by a member in the AS.
The security requirements include:

Sender ambiguity: The probability that a verifier successfully determines the real sender of the anonymous message is exactly 1=n, where n is the total number of members in the AS.

Unforgeability. An anonymous message scheme is unforgeable if no adversary, given the public keys of all members of the AS and the anonymous messages m_1, m_2,.. m_n adaptively chosen by the adversary, can produce the message. The main idea is that for each message m to be released, the message sender, or the sending node, generates a source anonymous message authenticator for the message m. The generation is based on elliptic curves. For a ring signature, each ring member is required to compute a forgery signature for all other members in the AS.

Suppose that the message sender (say User1) wishes to transmit a message m anonymously from her network node to any other nodes. The AS includes n members, A1,A2, ... ,An, for example, S={A1,A2, ... ,An}, where the actual message sender Alice is At, for some value t; 1 <= t <= n. In this experimental system, we will not distinguish between the node Ai and its public key Qi. Therefore, we also have S={Q1, Q2, ...,Qn}.

Authentication Generation Algorithm: Suppose m is a message to be transmitted along with base station node id. The private key of the message sender User1 is dt; 1 <= dt <= n. To generate an efficient scheme for message m, User1 performs the following steps:

Algorithm 3.1: Authentication Generation Algorithm

//For User1 to sign a message **m**

1. Select a random hop level integer H_A, $1 \le H_A \le N \le 1$.

2. Calculate total hop level with total terminal client node N1

3. Select a random integer k_A, $1 \le kA \le N \le 1$.

4. Calculate $r = x_A \bmod N$ & $H_A \bmod N_1$, where x_A; $y_A = k_A G$. If r = 0,

go back to step 1.

5. Calculate $h_A \leftarrow h(m, r)$, where h is a cryptographic hash function, such as SHA-1, and ← l denotes the l leftmost bits of the hash.

6. Calculate $h_A \leftarrow G(m, r)$, where h is a cryptographic hash function, such as SHA-1, and ← l denotes the l leftmost bits of the hash.

7. Calculate $s = rd_A h_A + kA \bmod N$.If s = 0,

go back to step 2

8. The signature is the pair (r1, s1).

EXPERIMENTS AND FINDINGS

The experimental result for secure transmission node analysis of existing system contains number of time slot interval in minutes and by using that given time interval, the average ratio of secure transmission node's percentage will be detected.

IV. CONCLUSION

This research work proposed to use message sending, a physical property associated with each wireless device that is hard to falsify and not reliant on cryptography as the basis for detecting multiple attackers in wireless networks. It provided theoretical analysis of using the hop by hop based inherited from wireless nodes for attack detection. The approach can both detects the presence of attacks as well as determine the number of adversaries we can localize any number of attackers and eliminate them.

In addition, a Multi hop-based node message sending and compromise detection scheme is proposed using

the Global Elliptic Curve Cryptography (GECC). Furthermore, several possible attacks are described against the proposed scheme and proposed multi hop based measures against these attacks. The scheme is evaluated in simulation under various scenarios. The experimental results show that the scheme quickly detects untrustworthy multi hop with a small number of trust reports.

In future, the scheme may evaluate against various types of attacker models. It is believed that a game theoretic model is suited for this evaluation. A variety of strategies may be studied that may be taken by detector and adversary.

- The application if developed as web services, then many applications can make use of the records.
- The data integrity in cloud environment is not considered. The error situation can be recovered if there is any mismatch.
- The web site and database can be hosted in real cloud place during the implementation.

REFERENCES

[1] D. Pointcheval and J. Stern, "Security Proofs for Signature Schemes," Proc. Advances in Cryptology (EUROCRYPT), pp. 387-398, 1996.

[2] M. Reiter and A. Rubin, "Crowds: Anonymity for Web Trans-action," ACM Trans. Information and System Security, vol. 1, no. 1, pp. 66-92, 1998.

[3] H.Chan and A. Perrig, "Security and Privacy in Sensor Networks," IEEE Computer, October 2003.

[4] Akyildiz, W. Su, Y. Sankarasubramaniam, and E.Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, March 2002.

[5] Larose D.T., Discovering knowledge in data: an introduction to data mining, Wiley-Interscience, 2005.