ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

A Secure Intrusion Avoidance System Using Hybrid Cryptography

N.Poornima[1], M.O.Ramya[2,] M.Vinotha[3,] K.Kalaiselvi

[1]UG student, Department of CSE, SNS College of engineering,, India.

[2]UG student Department of CSE, SNS College of engineering,, India.

[3]UG student, Department of CSE, SNS College of engineering,, India.

Assistant professor ,Department of CSE, SNS College of engineering,, India.

ABSTRACT - In MANET, we considered solid secrecy requirements regarding secrecy-maintain. For that propose an unobservable secure routing scheme Solid hybrid security protocol to offer an authorised content accessibility and complete unlinkability. Solid hybrid security protocol is uses a combination of group signature and ID-based encryption for the secure route finding. Security analysis described about that solid hybrid security protocol can well protect user privacy against the both inside and outside attackers. For MANET we define stronger privacy requirements regarding privacy-preserving routing. For that an unobservable secure routing scheme USOR has been proposed to offer complete unlinkability and content unobservability for all types of packets. USOR is an efficient combination of group signature and ID-based encryption for route discovery. Security analysis demonstrates that USOR can well protect user privacy against both inside and outside attackers. It implements USOR on ns2, and evaluates its performance by comparing with AODV and EAACK. The simulation results show that USOR has satisfactory performance compared to AODV, but also achieves stronger privacy protection than existing schemes like EAACK.

I. INTRODUCTION

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue
operations, disaster relief efforts, and military networks. For providing secure transmission in the military environment USOR is used as a routing protocol. The USOR is enhanced from the EAACK.

II. EXISTING SYSTEM

EAACK

This scheme was proposed by Elhadi M. Shakshuki [1].it is the advanced scheme from AACK [3]. It is the combination of ACK, S-ACK, MRA and Digital signature using DSA.

A. ACK

ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. Whenever it cannot able to detect it moves to S-ACK

B. S-ACK

The S-ACK scheme is an improved version of the TWOACK. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to

detect misbehaving nodes in the presence of receiver collision or limited transmission power.

C. MRA

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. By the using MRA scheme, EAACK was able to detect malicious nodes despite the existence of false misbehavior report.

D. Digital Signature

EAACK is an acknowledgment-based IDS. All the above parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all fully based on acknowledgment packets to detect misbehaviors in the network. Thus, it is very important to ensure that all acknowledgment packets in EAACK are authentic.

If the attackers are able to send the false acknowledgment packets, all of the three schemes will be vulnerable. With regard to this concept, existing system used the digital signature along with the DSA. But the existing system cannot able to reduce the network overhead caused by digital signature.

The existing system cannot be used for military application. To use in a military application we proposed a scheme USOR routing protocol.

III. PROPOSED SYSTEM

The proposed system initially implements the key generation, Groupid sharing and leader selection after. After the completion of route discovery transmission will done between the source and destination by using encryption and decryption.

The following are the sample screen shot to show the implementation of USOR and the performance over packet delivery ratio and network overhead

The following are the step by step procedure followed in proposed system.

Step1:

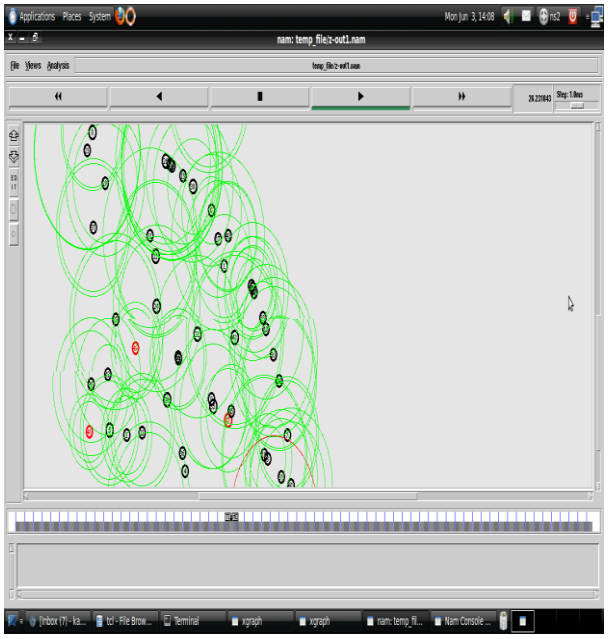
ENTERING PUBLIC KEY AND PRIVATE KEY FOR SOURCE SIDE

Step2:

ENTERING PUBLIC KEY AND PRIVATE KEY FOR DESTINATION SIDE

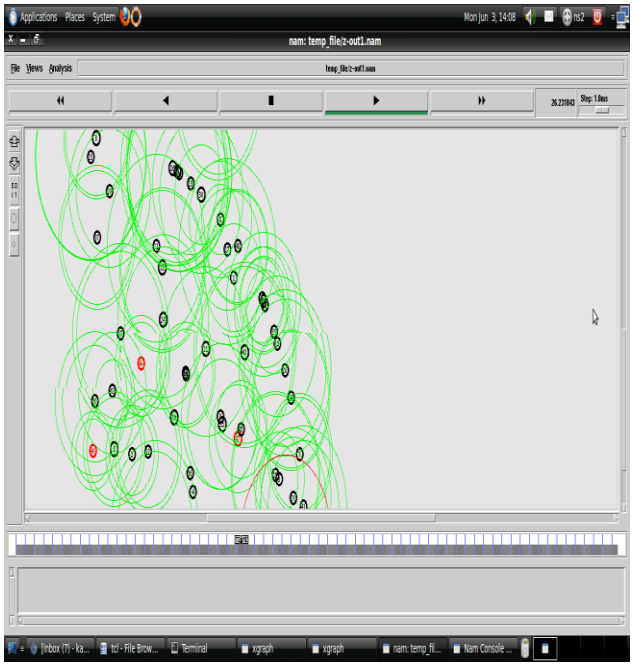
Step3:

SENDING RREQ



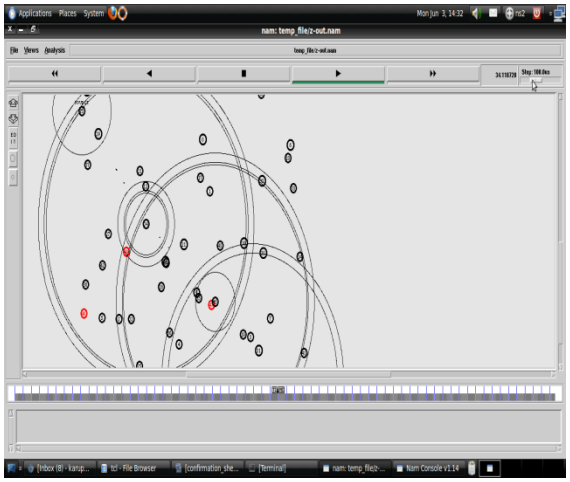
Step 4:

GENERATING RREP



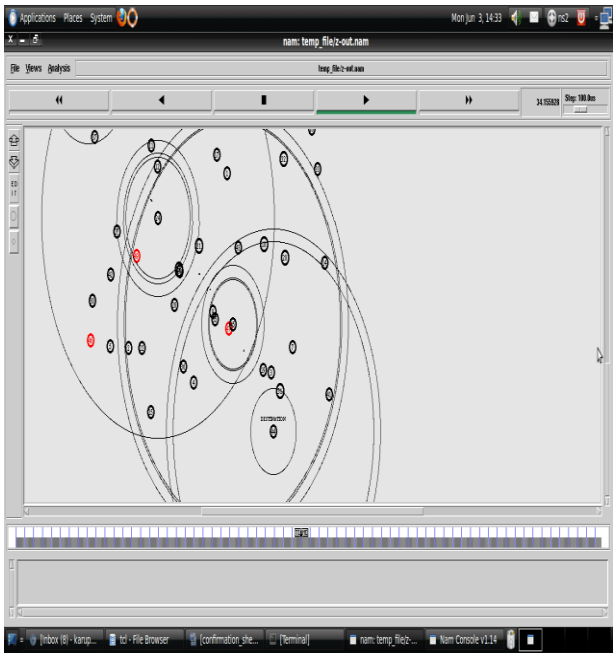
Step5:

SELECTING THE PATH WHICH HAVING GROUP ID



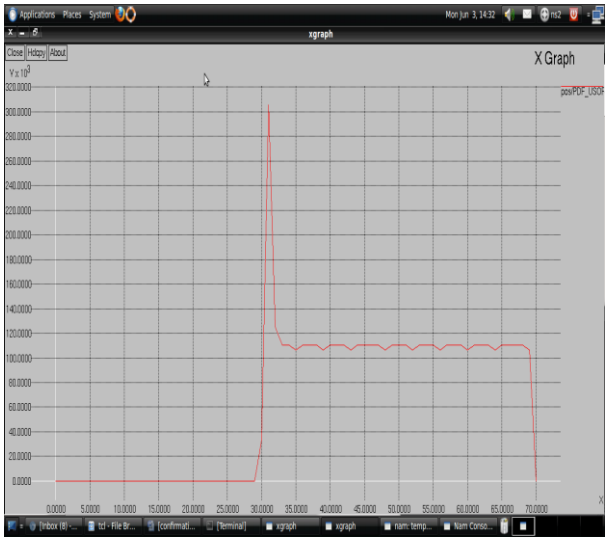
Step6:

DESTINATION RECEIVING THE DATA FROM SELECTED PATH



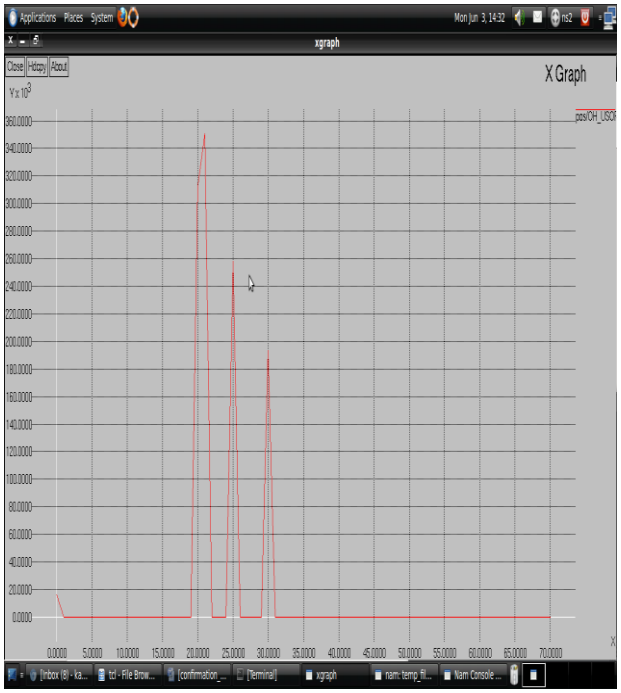
Step 7:

PACKET DELIVERY FUNCTION



Step 8:

NETWORK OVER HEAD



DIGITAL SIGNATURE

The existing system uses the DSA in digital signature. Since it is based on public key alone we use RSA in the proposed system to enhance the security level. The proposed system consist of two parts RSA and SHA-1(message digest).

RSA *(*algorithm*)*

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman[5].

A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. This RSA used for the encryption and decryption process.

Example:

1. Choose two distinct prime numbers, such as p and q
2. Compute $n = pq$
3. Compute the product as

   $\varphi(n) = (p-1)(q-1)$
4. Choose any number $1 < e < 3120$ that is coprime to 3120. Choosing a prime number for e leaves us only to check that e is not a divisor of 3120.
5. Compute d, the modular multiplicative inverse of e (mod $\varphi(n)$) yielding

SHA (algorithm**)**

In cryptography, **SHA-1** is cryptographic hash function designed by the United States National Security Agency and published by the United States NIST as a U.S. Federal Information Processing Standard. SHA stands for "secure hash algorithm". The four SHA algorithms are structured differently and are distinguished as *SHA-0*, *SHA-1*, *SHA-2*, and *SHA-3*. SHA-1 is very similar to SHA-0, but

corrects an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-2 on the other hand significantly differs from the SHA-1 hash function.

SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols.

SHA-1 produces a 160-bit message digest based on principles similar to those used by Ronald L.Rivest of MIT in the design of the MD4 and MD5 message digest algorithms, but has a more conservative design.

The original specification of the algorithm was published in 1993 as the *Secure Hash Standard*, FIPS PUB 180, by U.S. government standards agency NIST (National Institute of Standards and Technology). This version is now often referred to as *SHA-0*. It was withdrawn by NSA shortly after publication and was superseded by the revised version, published in 1995 in FIPS PUB 180-1 and commonly referred to as *SHA-1*. SHA-1 differs from SHA-0 only by a single bitwise rotation in the message schedule of its compression function; this was done, according to NSA, to correct a flaw in the original algorithm which reduced its cryptographic security. However, NSA did not provide any further explanation or identify the flaw that was corrected. Weaknesses have subsequently been reported in both SHA-0 and SHA-1. SHA-1 appears to provide greater resistance to attacks, supporting the NSA's assertion that the change increased the security.This SHA-1 is used for creating message digest in digital signature.

LEADER NODE SELECTION

This will used to elect a leader node among the group and sharing the Groupid to the members present inside the jammer area. The jammer is considered to use our concept in the military application apart from the commercial application. Thus the EAACK cannot use in military application but this system can do. The process of leader node selection and sharing of Groupid done by the use of following algorithm

Algorithm

1. Initialize the nodes as follows
    a. Leader node: (it can share the key at initial time)
    b. Normal node: (normal mobile node)
2. Leader node initially sends the Group ID key to all then mobile node
3. If normal node received that ID then stores into memory
4. If node having GID
    a. It can access the request
5. If not
    a. Can't access the request
6. If node (i) wants to communicate with another node
    a. Node i generates the hash code(by sha-1)
    b. Encrypting (by RSA) that code with private key of node i
    c. And sends to destination node
7. destination node can verify that encrypted message by using the public key and as well as group ID
    a. if match
        i. node j sending own code to source node i
    b. if not match
        i. ignore
8. if match code of node j
    a. transfer the data
9. if not match
    a. ignore

IV.RESULT AND DISCUSSION

Hence the proposed system shows better result in increasing packet delivery ratio and reducing network overheard even though the number of hackers increased in the simulation. When compared with the existing system EAACK the USOR contain same number of normal nodes along with increased hackers it shows the better result.

V.CONCLUSION

The proposed system USOR based on group signature and ID-based cryptosystem for ad hoc networks is proposed. The design of USOR offers strong privacy protection—completes unlinkability and content unobservability for ad hoc networks. The security analysis demonstrates that USOR not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. We implemented the protocol on ns2 and examined performance of USOR, which shows that USOR has satisfactory performance in terms of packet delivery ratio, latency and normalized control bytes.

REFERENCES

[1].EAACK—A Secure Intrusion-Detection
System for MANETs Elhadi M. Shakshuki, *Senior Member, IEEE,* Nan Kang, and Tarek R. Sheltami, *Member,* IEEE transactions on industrial electronics, vol. 60, no. 3, march 2013

[2] D. Johnson and D. Maltz, *"Dynamic Source Routing in ad hoc wireless networks*," in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5,pp. 153–181.[3] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, *"An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput.*, vol. 6, no. 5,pp. 536–550, May 2007.

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, *"Mitigating routing misbehaviourin mobile ad hoc networks,"* in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw*., Boston, MA, 2000, pp. 255–265.

[5] R. Rivest, A. Shamir, and L. Adleman, *"A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1983.

[6]Model Checking Ad Hoc Network Routing Protocols: ARAN vs. endairA Davide Benetti Massimo Merro Luca Vigan`o Dipartimento di Informatica, Universit`a degli Studi di Verona, Italy

[7] An Identity-free and On Demand Routing Scheme against Anonymity Threats in Mobile Ad-hoc Networks Jiejun Kong∗ Xiaoyan Hong† Mario Gerla‡∗ Scalable Network Technologies, Inc. †Dept. of Computer Science ‡Dept. of Computer Science 6701 Center Drive West, Suite 520 University of Alabama University of California Los Angeles, CA 90045 Tuscaloosa, AL 35487 Los Angeles, CA 90095