RESEARCH ARTICLE OPEN ACCESS

Providing Authentication in Wireless Network to Prevent Jamming Attacks

R.Akila[1], T.J. Jeyaprapha[1,] Dr. G. Sumathi[2]

([1]Department of Electronics and Communication Engineering, R.Akila, M.E final year, Sri Venkateswara College of Engineering, Sriperumbudur)

([1]Department of Electronics and Communication Engineering, T.J.Jeyaprabha, Assistant Professor, Sri Venkateswara College of Engineering, Sriperumbudur)

([2]Department of Information and Technology, Dr.G.Sumathi, Head-IMS, Professor, Sri Venkateswara College of Engineering, Sriperumbudur)

ABSTRACT
Wireless and mobile networks represent an increasingly important segment of networking research as a whole, driven by the rapid growth of portable computing, communication and embedded devices connected to the internet. Goal of the process is to bring privacy in any conversation between nodes in a network and to provide security from the attackers. The need of bringing privacy is to defend ourselves from any of the attacks in wireless network. AODV is a message of routing messages between mobile computers and it allows these mobile computers or nodes to pass messages through their neighbors to nodes with which they cannot directly communicate. Here, we propose RSA technique for providing authentication for data and control packets. By using this technique we provide the authenticated data transmission and also to prevent the damage in the network by the attackers.

Keywords – AODV (Ad hoc On-demand Distance Vector), RSA (Ron_Rivest, Adi_Shamir and Leonard Adleman.

I. INTRODUCTION

The most common wireless technologies use radio. With radio waves distances can be short, such as a few meters for television or as far as thousands or even millions of kilometers for deep-space radio communications. It encompasses various types of fixed, mobile, and portable applications, including two, cellular telephones, personal digital assistants (PDAs), and wireless networking.

Overall, it is clear that mobile, wireless and sensor devices will certainly outnumber wired end-user terminals on the Internet in the near future, strongly motivating consideration of fundamentally new network architectures and services to meet.

More than 90% of all oral cavity cancers are Oral Squamous Cell Carcinoma (OSCC),

Changing needs. Over the next 10-15 years, it is anticipated that significant qualitative changes to the Internet will be driven by the rapid proliferation of mobile and wireless devices, which may be expected to outnumber wired PC's as early as 2010. The potential impact of the future wireless Internet is very significant because the network combines the power of computation, search engines and databases in the background with the immediacy of information from mobile users and sensors in the foreground. Wireless connections are by nature significantly less stable than wired connections.

When a malicious node D'intercepts the data traffic from the source node *S* to the destination node *D,* a black hole attack takes place. D' may misbehave by agreeing to forward packets but fail to do so, because it is overloaded, selfish, malicious, or broken**.** This kind of black hole attack can be detected by setting the promise mode of each node. In this system they proposed a novel approach, Topology Graph-Based Anomaly Detection (TOGBAD), for detecting routing attacks in tactical MANETs [1].A selfish behaviour threatens the entire community. This paper proposes a selfishness prevention protocol for open MANETs. The drawback of this is it works only on early stages of development and lacks theoretical and experimental validation [2]. The watchdog method**,** detects misbehaving nodes acting alone by maintaining a buffer that contains recently sent packets. When a node forwards a packet, the node's watchdog ensures that the next node in the path also forwards the packet; the watchdog does this by listening to the next node promiscuously. If the next node does not forward the packet then it is termed as misbehaving. In this scheme, every packet that is overheard by the watchdog is compared with the packet in the buffer to see if there is a match. A match confirms that the

packet has been successfully delivered and it is removed from the buffer. If a packet has remained in the buffer beyond the timeout period then a failure tally for the node responsible for forwarding the packet is incremented. If this tally exceeds a predetermined threshold then the node is termed as malicious and the network is informed accordingly [3]. Two conceptual models for charging for the packet forwarding service. In the first one, called Packet Purse Model, the source of the packet is charged, whereas in the second one, called Packet Trade Model, the destination is charged. The two models can also be combined to provide a hybrid solution. We believe that introducing a kind of virtual currency can serve several other purposes in mobile ad hoc networks. First, it can be used to remunerate not only communication services, as described in this paper, but also information services. Second, it can be used as a way to pay for the usage of backbones or satellite links, when a node has to communicate with a very distant party. In this case, the virtual currency will have to be converted in some way into "hard" currency [4].several algorithms are proposed to detect the black hole attack like DSR, AODV, TORA, DSDV, STAR etc. Proposed two solutions first, isolate the misbehaving nodes from the actual routing protocol for the network. But it adds complexity to protocol. Second, it detects only if the receiver's network interface is accepting packets, but they otherwise assume that routing nodes do not misbehave. Although trusting all nodes to be well behaved increases the number of nodes available of routing, it also admits misbehaving nodes to the network [5]. In this paper, the former are intended to enforce the cooperation by first detecting the selfish nodes, avoiding routing through them, and then punishing them via spreading their bad reputations and thus isolating them. This paper proposed a Secure Incentive Protocol (SIP) to motivate packet forwarding in totally self organizing MANETs without relying on any centralized infrastructure [6].Malicious nodes can intentionally alter routing messages and cause Denial-of-Service attacks, or can cause packet flooding to power down the network by successive broadcasting of Route Requests, or send periodic wake up calls or false alarms to neighboring nodes. This paper proposed a framework to eliminate colluding black hole attacks in the Ad hoc On-demand Distance Vector (AODV) routing protocol [7].

II. PROPOSED SYSTEM

Ad hoc On-demand Distance Vector (AODV) is a method of routing messages between nodes. It allows these mobile computers, or nodes, to pass messages through their neighbors to nodes with which they cannot directly communicate. AODV does this by discovering the routes along which messages can be passed. AODV makes sure these routes do not contain loops and tries to find the shortest route possible. AODV is also able to handle changes in routes and can create new routes if there is an error. Here we used the distance based process and it is for the non centralized process.

Here we propose RSA Technique for providing authentication for data and control packets. By using this technique we provide the authenticated data transmission and to avoid the damage in the network by the attackers. We use the Ad hoc On-demand Distance Vector (AODV) protocol for routing. High speed of encryption and Private Key is used. The authentication is a key barrier in the network information system security field. RSA is a open network environment technology, using public key cryptography system theory has implemented and supplied a universal security infrastructure for security services; it has two main applications, include encryption and digital signature.

III. Ad hoc On-demand Distance Vector (AODV)

The Ad hoc On-demand Distance Vector (AODV) routing protocol is intended for use by mobile nodes in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network. It uses destination sequence numbers to ensure loop freedom at all times (even in the face of anomalous delivery of routing control messages), avoiding problems (such as "counting to infinity") associated with classical distance vector protocols.

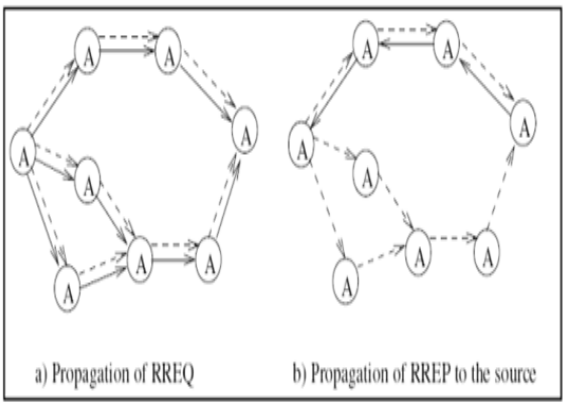

Fig.1. AODV Route discovery

One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom

and is simple to program. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest sequence number.

IV. RSA

RSA is a cryptosystem, which is known as one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm. 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. Breaking RSA encryption is known as the RSA problem. It is an open question whether it is as hard as the factoring problem.

The RSA algorithm involves three steps: key generation, encryption and decryption.RSA involve *public key* and a *private key*. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
   - ✓ For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.
2. Compute $n = pq$.
   - ✓ n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co prime.
   - ✓ e is released as the public key exponent.
   - ✓ e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.
5. Determine d as $d^{-1} \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).
   - ✓ This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$
   - ✓ This is often computed using the extended Euclidean algorithm. Using the pseudo code in the *Modular integers* section, inputs a and n correspond to e and t, respectively.
   - ✓ d is kept as the private key exponent.

The *public key* consists of the modulus n and the public (or encryption) exponent e. The *private key* consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.

ENCRYPTION

Alice transmits her public key *(n, e)* to Bob and keeps the private key secret. Bob then wishes to send message M to Alice. He first turns M into an integer m, such that $0 \le m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text c. This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice. Note that at least nine values of m will yield a cipher text c equal to m,[note 1] but this is very unlikely to occur in practice.

DECRYPTION

Alice can recover m from c by using her private key exponent d via computing

$$m \equiv c^d \pmod{n}$$

Given m, she can recover the original message M by reversing the padding scheme.

SIGNING MESSAGES

Suppose Alice uses Bob's public key to send him an encrypted message. In the message, she can claim to be Alice but Bob has no way of verifying that the message was actually from Alice since anyone can use Bob's public key to send him encrypted messages. In order to verify the origin of a message, RSA can also be used to sign a message.

Suppose Alice wishes to send a signed message to Bob. She can use her own private key to do so. She produces a hash_value of the message, raises it to the power of d (modulo n) (as she does when decrypting a message), and attaches it as a "signature" to the message. When Bob receives the signed message, he uses the same hash algorithm in conjunction with Alice's public key. He raises the signature to the power of e (modulo n) (as he does when encrypting a message), and compares the resulting hash value with the message's actual hash value. If the two agree, he knows that the author of

the message was in possession of Alice's private key, and that the message has not been tampered with since.

In the basic communication scenario, there are two parties, Alice and Bob, who want to communicate with each other. A third party, Eve, is a potential eavesdropper. RSA encryption, supplies unique and stability technology advantages, presents an authentication system.

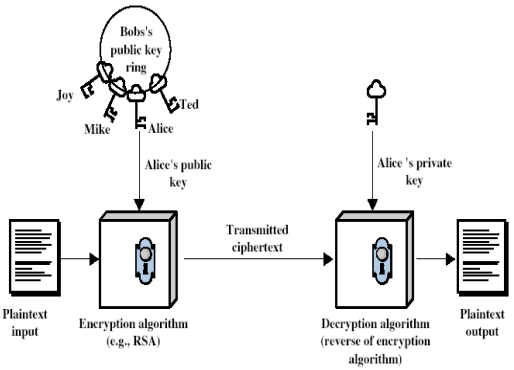

FIG. 2. RSA ENCRYPTION AND DECRYPTION

With a public key (PKA) or asymmetric key algorithm, a pair of keys is used. One of the keys, the private key, is kept secret and not shared with anyone. The other key, the public key, is not secret and can be shared with anyone. When data is encrypted by one of the keys, it can only be decrypted and recovered by using the other key.

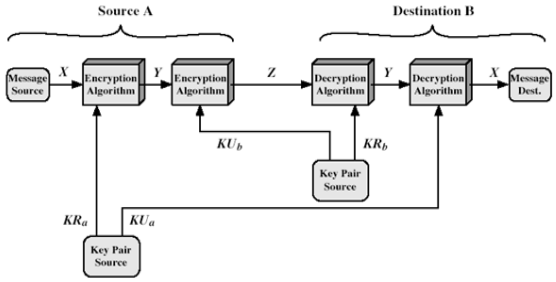

Fig.3. Public key cryptosystem: Secrecy and Authentication

V. RESULTS

The simulation work has been done with the Network Simulator ns-2, Version 2.29. In the simulation 100 nodes are randomly distributed within the network field of size 1000m * 1000m. Then vary the node speed from 5m/s to 30m/s.

MODULES LIST

The block diagram of this project has built by using five modules and they are 1.Network formation: the wireless network is formed with the multiple nodes. 2. Route Discovery: the identification of path between the source and the destination for the transformation of information's is done here. 3. Algorithm Implementation: the algorithm known as AODV is implemented for the route discovery.

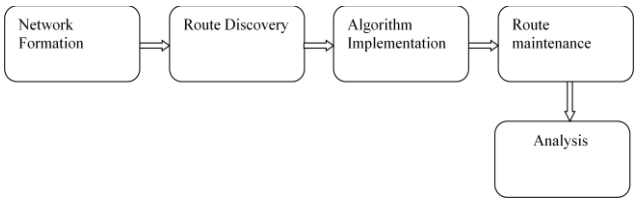

FIG.4. BLOCK DIAGRAM

4. Route Maintenance: RSA technique is introduced for providing the security between the sender and receiver for communication.
5. Analysis: Finally the performance like delay, throughput and packet delivery ratio is analyzed.

Let us focus on the performance of this routing protocol. We evaluated the performance of AODV as a routing protocol and RSA as algorithm for authentication using NS2. By implementing the another routing protocol and algorithm for authentication, the performance comparison will be done by comparing the end to end delay, overall delay, throughput, packet delivery ratio.

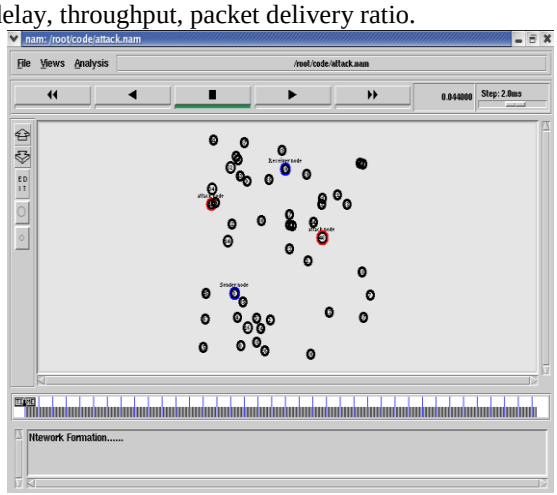

FIG.6. Sender and receiver node in a network with the attacker node

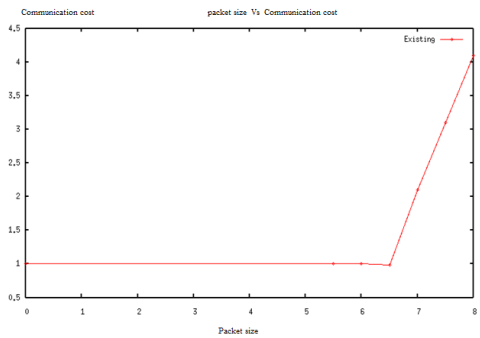

FIG.9. Packet size Vs communication cost

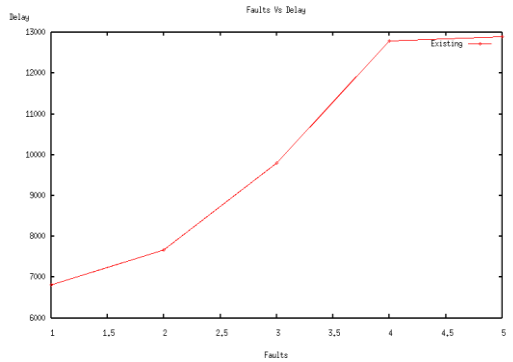

FIG.10. Fault Vs delay

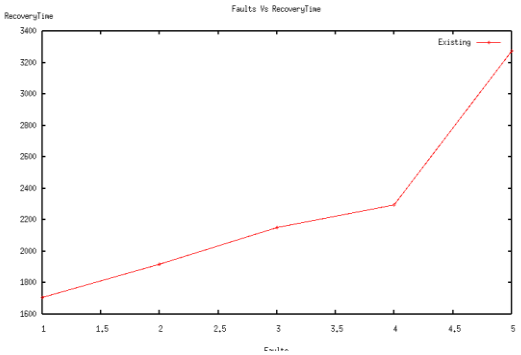

FIG.11. Fault Vs recovery time

VI. CONCLUSION

In this paper, we proposed RSA Technique for providing authentication for data and control packets. By using this technique we provide the authenticated data transmission and to avoid the damage in the network by the attackers. We use the Ad hoc On-demand Distance Vector (AODV) protocol for routing. In future work thus with the OLSR routing protocol based on the identification of poor link stability we adjusting the route discovery process for improving the route finding method. Also EDH will be used as a cryptographic technique. Finally the results like throughput, delay, packet loss can be compared to find the best technique.

REFERENCES

[1] Elmar Gerhards-Padilla, Nils Aschenbruck, Peter Martini, Marko Jahnke, Jens T¨olle ,“ Detecting Black Hole Attacks In Tactical Manets Using Topology Graphs”, IEEE conference on local computer Networks,15-18 Oct.2007.

[2] Hugo Miranda Lu´ıs Rodrigues , “Preventing Selfishness In Open Mobile Ad Hoc Networks”, In the proceedings of Distributed Computing systems, pages- 440 – 445, 19-22 May 2002.

[3] Animesh Patcha and Amitabh Mishra , “Collaborative Security Architecture For Black Hole Attack Prevention In Mobile Ad Hoc Networks”, In the proceedings of Radio and Wireless Conference, pages- 75 – 78, 10-13 Aug. 2003.

[4] Levente Butty_an and Jean-Pierre Hubaux, “**Nuglets**: A Virtual Currency To Stimulate Cooperation In Self-Organized Mobile Ad Hoc Networks”, 2001.

[5] Sergio marti, T.J.Giuli, Kevin lai, and Mary Baker, “Mitigating Routing Misbehavior In Mobile Ad Hoc Network”, 2000.

[6] Yanchao Zhang, Wenjing Lou, Yuguang Fang,” A SECURE INCENTIVE PROTOCOL FOR MOBILE AD HOC NETWORKS”, 2004.

[7] Ramaswami, S.S, Upadhyaya, S,”SMART HANDLING OF COLLUDING BLACK HOLE ATTACKS IN MANETs AND WIRELESS SENSOR NETWORKS USING MULTIPATH ROUTING”, pages- 253 – 260,21-23 June 2006.