International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 12, ISSN No. 2455-2143, Pages 25-28
Published Online October-November 2016 in IJEAST (http://www.ijeast.com)

MUTUAL AUTHENTICATED KEY AGREEMENT SCHEME FOR INTEGRATED INTERNET MANETS

Arshad Ahmad Khan Mohammad
Assistant Professor, NCET,
Hyderabad, India

C Atheeq
Assistant Professor, DCET,
Hyderabad, India

***Abstract*— With the support of integrating internet with MANETS, it offers communication extension scenarios where secure data transmission is challenging as other resource constraint networks. In this work, we develop a new Mutual Key agreement mechanism using RSA in which the key agreement happens between fixed node in internet and mobile node in MANETs with the help of gateway. Key generation is initiated with gateway, and our mechanism aim is to reduce the key management cost over mobile node, as MANETs is a resource constrained environment. We implemented the proposed mechanism with the help of NS2. Simulation results shows that our mechanism provide the mutual authentication between communication entities & abstained from various attacks**

Keywords—**MANETs, Integration, IIM, RSA, Mutual authentication, Key agreement**

I. INTRODUCTION

MANETs [1-6] is wireless multi hop communication network composed of wireless heterogeneous mobile devices communicating each other without infrastructure. Most important characteristic of MANETs is adaptability, heterogeneity & dynamic nature. The feature of MANETs [2] includes, easy to deploy, cost/time effective. Applications of MANETs are military, law enforcement, conferencing, environment monitoring & vehicular communication. Due to its characteristics, features & applications there is increasing demand towards integrating MANETs with internet, which increases the application domain of MANETs & allows the network expansion. Integration between MANETs & internet is known as IIM (Integrated Internet mobile ad hoc networks) & it is achieved by the device called gateway.

In IIM environment, mobile node present in a MANETs access the internet from fixed node present in a infrastructure based network through gateway. Due to MANETs [3] characteristics, there is high desirability of authentication. Mobile node need to authenticate itself with fixed node in order to get internet access. Authentication is a way to provide secure communication in any network environment. To provide authentication, fundamental requirement is to generate a key between communicating parties [4].

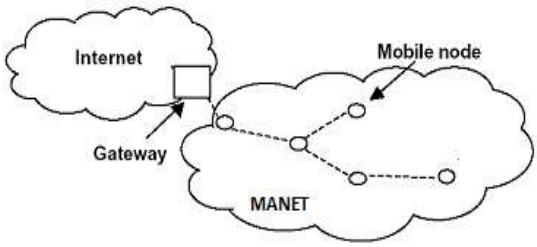

Fig. 1 Integration of Internet and MANET

RSA is a well-known key generation algorithm to generate & agree key between source and destination securely. In this paper we use RSA to provide authentication between mobile node in MANETs & fixed node in infrastructure based network. The remaining paper organized as follows in section 2 we describe the RSA algorithm, our proposed model explained in section 3 our work ends with performance analysis and conclusion.

II. RSA

RSA [7] is the most popular and proven an asymmetric key cryptography algorithm as it uses two different keys for encryption and decryption the data by authenticating the nodes. It generates two keys private key and public key. In this system, encryption is done with the help of public key and the decryption key is kept secret. Private key is the secret key that is generated at the node and public key is known to other parties who wants to interact with the node. For this reason it is also known as public key cryptography. It is based on factoring product of two large prime numbers. The basic principle behind RSA is the observation that it is practical to find three very large positive integers' e, d and n such that with modular exponentiation for all m:

$$(m^e)^d \equiv m \bmod(n)$$

and that even knowing e and n or even m it can be extremely difficult to find d. Additionally, for some operations it is convenient that the order of the two exponentiations can be changed and that this relation also implies

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 12, ISSN No. 2455-2143, Pages 25-28
Published Online October-November 2016 in IJEAST (http://www.ijeast.com)

$$(m^d)^e \equiv m \bmod(n)$$

The key can be distributed by enabling mobile node to send its encrypted messages, fixed node transmits its public key (n, e) to mobile node via gateway. The private key d is never distributed

Encryption

Suppose that Mobile node (MN) would like to send message M to Fixed node (FN).

MN first turns M into an integer m, such that $0 \leq m < n$ and gcd(m, n) = 1 (that is, m and n are co-prime integers) by using an agreed-upon reversible protocol known as a padding scheme. It then computes the cipher text c, using Fixed node's public key e, corresponding to

$$c \equiv m^e \bmod(n)$$

This can be done reasonably quickly, even for 500-bit numbers, using modular exponentiation. Mobile node then transmits c to fixed node

Decryption

Fixed node can recover m from c by using its private key exponent d by computing

$$c^d \equiv (m^e)^d \equiv m \bmod(n)$$

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

Key generation

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 similar in magnitude but 'differ in length by a few digits' to make factoring harder. Prime integers can be efficiently found using a primarily 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 $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n - (p + q - 1)$, where φ is Euler's totient function. This value is kept private.
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.
5. Determine *d* as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., *d* is the modular multiplicative inverse of *e* (modulo $\varphi(n)$)

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*.

III. PROPOSED ALGORITHM

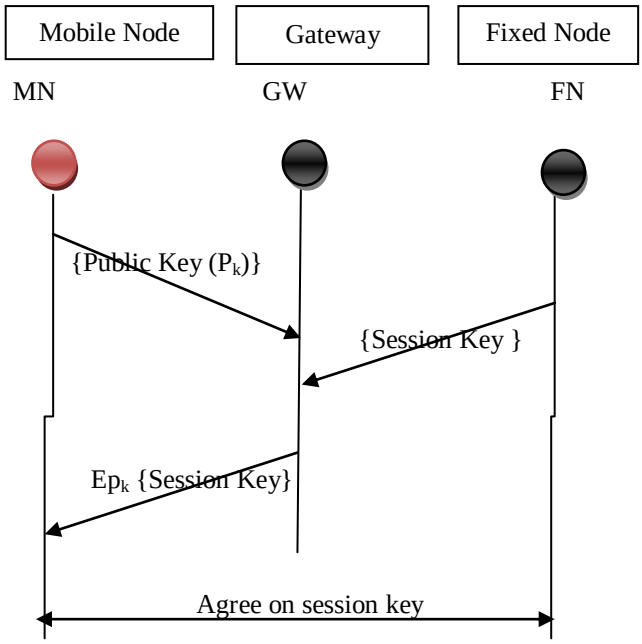

Fig 2. Session key agreement algorithm

The mobile node (MN), which want to communicate or access the internet with fixed node present in a internet need to agree a shared key 'K_s' with gateway with the help of RSA [7] algorithm. All fixed nodes connected with gateway need to agree on a common key known as gateway key (K_g) with the help of diffei –helman algorithm [8]. We are avoiding overhead at MANETs by generating session key reactively i.e, whenever MN want to communicate at that time only it will agree the session key with gateway. For every new communication session key will get updated.

Algorithm

1. Whenever new node detects the gateway or

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 12, ISSN No. 2455-2143, Pages 25-28
Published Online October-November 2016 in IJEAST (http://www.ijeast.com)

node want to communicate/access the internet from fixed node present in a infrastructure based network, agree a encryption-decryption key with gateway with the help of RSA algorithm

2. Fixed node generate a session key and agree the this key with gate way with the help of diffei –helman key exchange algorithm
3. Now, gateway encrypt the session key with public key of node and send it to mobile node
4. Mobile node decrypt the message received by gate way and, retrieve the session key
5. Now the communication information between MN and fixed node is encrypt &/ decrypt by the help of session key

IV. PERFORMANCE ANALYSIS

We developed a proposed model using NS2 with necessary enhancement in NS2 libraries & analyze the performance of proposed model. We evaluated the overhead of proposed model with respect to mobility in Mobile nodes of MANETs (Random way point mobility model). For evaluation we have consider the scenario such a way that mobile node want to communicate with fixed node through gateway. The simulation parameters which we used to evaluate the performance of our proposed model is shown in table 1

Table -1 Simulation parameters of MANETs

Network Parameters	Values
Simulation Duration	100 s
Number of Nodes	20-90
Link Layer	Logical Link
MAC	802.11
Mobility	Random way point
Routing	Reactive
Radio Communication	Random way point
Queue	Drop-Tail priority
Application	CBR
Network Area	1200m x1 200m

We measure the computation overhead of RSA algorithm with respect to key size & we plotted the graph, which is shown in figure 3. Computation overhead is the one of the parameter is used to determine the security protocol. We implemented over protocol over AODV routing protocol, thus we compared the overhead of our proposed model with existing AODV model. Figure 4 clearly indicating that our proposed model does not greatly impact on computation overhead, and we can deploy security architecture with our proposed model with least overhead.

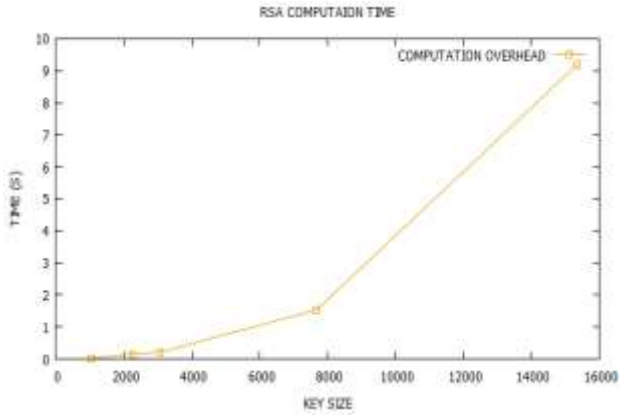

Fig 3. Computation overhead of RSA algorithm with Key size

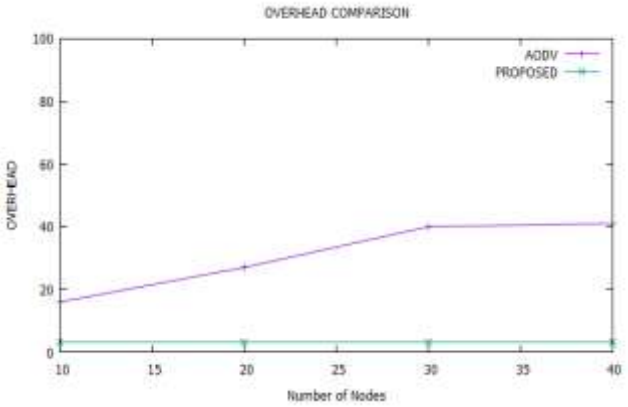

Fig 4. Computation overhead of proposed model with existing model

V. CONCLUSION

In this work, we introduced a key agreement protocol for integrated internet MANETs. Our protocol gives the way to securely agree a session key between mobile nodes in a MANETs with fixed node in an infrastructure based network with the help of gateway. Our mechanism uses a RSA algorithm for key agreement. Performance results show that our model can be deployed in a IIM network with least overhead

VI. REFERENCE

[1] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru. "Energy Aware Routing For Manets Based On Current Processing State Of Nodes." Journal of Theoretical & Applied Information Technology 91.2 (2016).

[2] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru. "Analytical Model for Evaluating the Bottleneck Node in MANETs." Indian Journal of Science and Technology 9.31 (2016).

[3] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Mohammed Abdul Razzak. "Reactive Energy Aware Routing Selection Based on Knapsack Algorithm (RER-SK)." Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2. Springer International Publishing, 2015

[4] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru. "Cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks." Indian Journal of Science and Technology 9.26 (2016).

[5] Sana, Afreen Begum, Farheen Iqbal, and Arshad Ahmad Khan Mohammad. "Quality of service routing for multipath manets." Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on. IEEE, 2015

[6] Siddiqua, Ayesha, Kotari Sridevi, and Arshad Ahmad Khan Mohammed. "Preventing black hole attacks in MANETs using secure knowledge algorithm." Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on. IEEE, 2015.

[7] Blömer, Johannes, Martin Otto, and Jean-Pierre Seifert. "A new CRT-RSA algorithm secure against bellcore attacks." Proceedings of the 10th ACM conference on Computer and communications security. ACM, 2003

[8] Kocher, Paul C. "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems." Annual International Cryptology Conference. Springer Berlin Heidelberg, 1996.