INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
(Volume2, Issue3)
Available online at: www.Ijariit.com

Trusted key management with RSA Based Security Policy for MANETS

Vandana Arora[1], Mr. Sunil Ahuja[2]

Student[1], Associate Professor[2]

Department Of Computer Science and Engineering, DIET, Karnal Haryana-132001

Abstract-A mobile ad hoc network (MANET) is a wireless communication network, which does not rely on any centralized management or a pre-existing infrastructure. Various key management authorities distributed over the network, each with a periodically updated share of the secrete key, is usually adopted. Thus many efforts have been made to adapt key management authority's tasks to the dynamic environments of MANETs and distribute the tasks of among MANET nodes. At present various cryptographic techniques are being deployed to meet the ever-changing needs, which compels to device unique security mechanism for MANET, enabling individual and corporate entities to protect the transmission of data without any intrusion by illegal means. Cryptographic techniques could be either of symmetric key cryptography and or asymmetric key cryptography or hash functions. Symmetric cryptosystem requires the existence of common shared secret key between two communicating nodes whereas asymmetric cryptosystem maintains unique key pair between any two communicating nodes (peers). An asymmetric cryptosystem is more efficient in a given task oriented key utilization process. In this mechanism, the private key needs to be kept secret with one entity but the authenticity of the corresponding public key for the same entity must be guaranteed somehow by a trusted third party In this paper, a novel mutual authentication and key management (agreement) protocol has been developed for one hop communication in mobile ad-hoc networks. The protocol has several salient features like mutual authentication, confidentiality, integrity and key agreement. The protocol utilizes RSA signature generation and verification algorithm.

Keywords- RSA Cryptosystem, AODV Based RSA Security, Trusted Key Management

I. WHAT IS MANET

A Mobile Ad-hoc web (MANET) is a sovereign collection of mobile routers or nodes conversing above wireless links. MANET is an unpredictable web lacking infrastructure. The wireless routers or nodes moves randomly and coordinate themselves arbitrarily. The nodes undeviatingly converse via wireless links inside every single other's wireless scope, as that are distant separately use supplementary nodes as relay in a multi-hop routing function. As the nodes are mobile, the construction of the web adjustments vibrantly and unpredictably above time. Ad-hoc webs are self-configuring and self-organizing, so to uphold contact amid nodes in the web, every single node behaves as a

transmitter, a host and a router. It is an autonomous arrangement of mobile hosts related by wireless links. There is no stationary groundwork such as center stations. If two hosts are not inside wireless scope, every single contact memos amid them have to bypass across one or extra intermediate hosts that deed as routers. These hosts move concerning randomly, therefore change the web topology alongside dynamism.

II. RELATED WORK

Hegland, A.M. et al, in "A survey of key management in ad hoc networks" 2006 [17], describe the wireless and dynamic nature of mobile ad hoc networks (MANETs) leaves them more vulnerable to security attacks than their wired counterparts. The nodes act both as routers and as communication end points. This makes the network layer more prone to security attacks. A main challenge is to judge whether or not a routing message originates from a trustworthy node. The solution thus far is cryptographically signed messages. This article surveys the classification of key management schemes based on contributory and distributive scheme. The analysis puts some emphasis on their applicability in scenarios such as emergency and rescue operations..

Young-Sik Hwang et al, in "The expansion of key infection model for dynamic sensor network" 2006 [18], describe the establishment of shared cryptography keys is one of the challenging problems in the sensor networks. Key infection (R. Anderson et al., 2004) is a promising model to solve this problem without complex mechanism on the commodity sensor networks. This model, however, does not consider the mobility of sensor, so it can not support dynamic sensor network fields. Therefore, key infection model has to be extended to handle the mobility of sensor, and then an extended key infection model can be used on the dynamic sensor network. In this paper, they propose a scheme to extend the key infection model for supporting dynamic sensor networks and explain how the proposed scheme is operated in detail. Also they prove that the proposed scheme is secure.

Boukerche, A. et al, in "A Secure Key Management Scheme for Wireless and Mobile Ad Hoc Networks Using Frequency-Based Approach: Proof and Correctness" 2008 [16],describe Security plays an important role in today's information technology, particularly in wireless and mobile environments due to the lack of pre-deployed infrastructure and the unsuitability of centralized management. Since the encryption technique has been introduced to provide secure communications, it is critical to manage all kinds of keys efficiently when the network size is large or the topology undergoes frequent changes. This paper presents a novel key management scheme that not only employs both symmetric and asymmetric key algorithms, but also achieves its key updates through a frequency-based approach. In addition, their scheme provides necessary protection for other aspects of key management, such as data confidentiality, key distribution, etc. Through the discussion of the current issues of key management and a further analysis of their key management scheme, their solution is proven to be secure in the process of key management and to be robust against attacks aimed at causing malicious key updates.

Raj Kamal Kapuret al.,(2015) [1] In this paper MANET is ad-hoc network in which mobile nodes co-operatively route the traffic to the nodes which are beyond their direct range. The mobile nodes are free to join or leave the network at will. The open architecture and dynamic topology coupled with lack of infrastructure make MANET vulnerable to variety of attacks at all layers. The secure transmission of data over MANET is a critical requirement. In this paper we have proposed a technique which provides secure transmission of data. The technique involves encryption of data using symmetric cryptographic technique, and also generating the digital signature of the data using the asymmetric cryptographic technique from the Hash of the data. The encrypted data is transmitted through the network to the destination where the received data and digital signature of the data are validated using symmetric and asymmetric cryptography. The data on validation is accepted thus ensuring secure data transmission. The proposed technique provides confidentiality, integrity, authenticity and non-repudiation to the data. It protects the data transmitted over the network from snooping, modification, replay and fabrication attack at the application layer.

III. PROPOSED METHODOLOGY FOR TRUSTED KEY MANAGEMENT

RSA is one of the early useful public-key cryptosystems and is extensively utilized for safeguard data transmission. In such a cryptosystem, the encryption key is area and differs from the decryption key that is retained secret. In RSA, this asymmetry is established on the useful difficulty of factoring the product of two colossal prime numbers, the factoring problem. RSA is made of the early messages of the surnames of Ron Rivest, Adi Shamir and Leonard

Adleman, who early openly delineated the algorithm in 1977. e. Breaking RSA encryption is recognized as the RSA problem; whether it is as hard as the factoring setback stays an open question.

GK (Group Key) is public by all cluster members. The keys in this are computed by deity node in NS-2 and given to Nodes in the MANET Scenario. Every single inner node key is utilized as a subgroup key for all descendent associates of the inner node. Prior to each safeguarded contact, nodes have to set up the features of the cryptography RSA (Key Creation Step). In our case we need exchanging identical keys GK. Area keys are utilized to encrypt the path. Parent node keeps the confidential key hidden in group. In our work we have made asymmetric keys exchanged above a safeguard contact channel.

Algorithm 1 :RSA Group Key Management in MANETs

1 Choose two distinct prime numbers p and q.
2 For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primarily test.
3 Compute n = pq.
4 n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
5 Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, where φ is Euler's quotient function. This value is kept private.
6 Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.
7 e is released as the public key exponent.
8 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.
9 Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the modular multiplicative inverse of e (modulo $\varphi(n)$).
10 This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$
11 This is often computed using the extended Euclidean algorithm. Using the pseudocode in the Modular integers section, inputs a and n correspond to e and $\varphi(n)$, respectively.
12 d is kept as the private key exponent.
13 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.

Algorithm 2 :Detection of RSA Paths

1 Initialize RSA Generation Process, by selecting p and q. p and q are initialized by bigint package in NS-2.
2 Initialize God Node for managing Public keys, Private Keys and Secure Paths.
3 Create Random flat grid based topology with given number of Nodes.
4 Add all nodes under God Node for Monitoring
5 During AODV routing Update God Encrypts Secure Path using public Key and generate Group key.
6 God Distributes the G_k to all known nodes so that in prior scenario can `decrypt path.
7 After receiving the first RREQ packet, the destination node waits for a short time period for any more RREQ packets, then chooses a path with the minimum hop count and sends a Route Reply (RREP) along the selected path. Each Node checks current path by decrypting the route/path while sending packet along the given path.
8 When a node wants to communicate to another node it first request the path available using route request. The secure path are encrypted in nature, So each node need to decrypt the path received by using its private key.
9 When a node is introduced in malicious path. Loss monitor tells that it has detected packet loss to god.
10 God responds by providing a new secured/trusted encrypted path. This new encrypted path contains only trusted nodes.
11 Only the trusted node can decrypt the path using the private key and reset its routing table and moves to a new secured path.
12 So with the help of God node a new secured path is generated and a new group key (Gk) is initialized.

In this paper we have counseled a RSA established cluster key association algorithm in MANETs. The work herein presents RSA established cluster key association algorithm alongside AODV protocol for allocation trusted and shorter routing trail in MANETs. This is the outstanding attainment in MANETs. The main goal of this work is to enhance throughput, packet transport ratio and conclude to conclude stay of the packet in the web.

IV. SIMULATION RESULT AND ANALYSIS

Network Simulator (Version 2), extensively recognized as NS2, is used here. Network Simulator (Version 2), extensively recognized as NS2, is plainly an event-driven simulation instrument that has proved functional in studying the vibrant nature of contact networks.

Table 1.1Simulation Parameter AODV Based RSA

Parameter	**Value**
Simulation Time(m-sec)	7500
Area	800x800
MAC Protocol	802.11
Routing Protocol	AODV, AODV RSA
Mobility Model	Random Way Point
Propagation Model	2-Ray Ground
Traffic Source	TCP/UDP
Seed[st.pt]	20
Transmission Range	300m
Node Placement	Random
Number of Nodes	18
Packet Queue	50

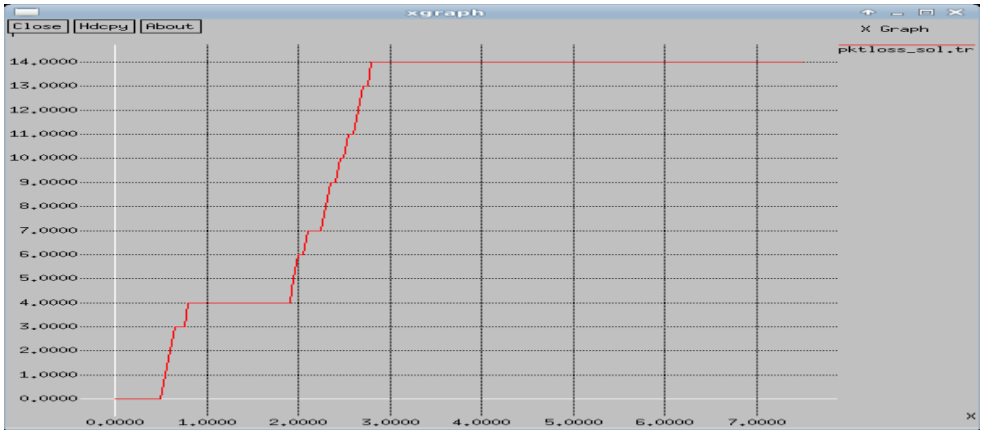

Figure: 1.1 Xgraph plotted for Packet Loss in AODV based RSA policy showing Stability after detection of Malicious node. On x-axis we have simulation time(sec) and on y-axis we have number of packets.

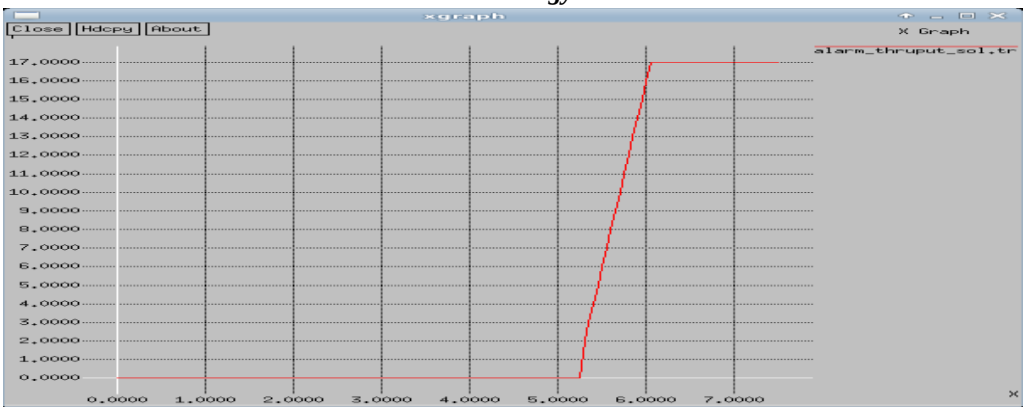

Figure 1.2 XGraph plotted for End to End Delay in AODV RSA based policy as soon as malicious node is detected End-end delay reduces to Zero. On x-axis we have simulation time and in y-axis we have End to End Delay for each node (ms).

V. CONCLUSION AND FUTURE WORK

In this paper, we present a new scheme to enhance security and gave the simulation to safeguard cryptographic RSA established key allocation scheme above mobile ad hoc web, established on the memo authentication scheme employing bilinear pairing. From the simulation consequence, it is discovered out that scheme works tremendously well in a tiny size of MANET. The Simulation we industrialized enhances the throughput of the channel on average75%, hence presentation of the channel is additionally enhanced as no of bits transferred are additionally increased. To accomplish more than 81% of presentation the web have to work on packet transferred have to be less than 1500 at each given instance. Technique proposed for RSA based group key management is completely decentralized. RSA based group key management algorithm with AODV protocol provides an efficient mechanism for allocation trusted and shorter routing path in MANETs. This is the great achievement in MANETs. Prior to any secured communication nodes must set up the details of cryptography (RSA). Thus improves the packet loss, end-end delay of packets as well as load on the node. In this serving, we furnish a little of the upcoming scrutiny association of our work. The work connected to RSA established cluster key association algorithm alongside AODV protocol to safeguard MANET. Area key cryptography is well-suited to random webs as it needs no a priori harmless key allocation method. Current improvements in RSA established cryptography incline to be permitting the utilization of area hidden algorithms in low-power devices. Motivated by our reasons upcoming we will work on a crypto arrangement employing an energy-efficient finished area hidden algorithm. Such protocol gave herein might give you the benefits of area hidden cryptography influential ad hoc area prop alongside purposes presently discovered just in symmetric systems. Additionally in upcoming we will familiarize a safeguard critical allocation arrangement predicated on quantum theory. Such algorithms can furnish protected method to allocate, or change the key that acknowledges each contain of the quantum contact channel.

VI. References

[1]. Kapur, Raj Kamal and Sunil Kumar Khatri. “Secure data transfer in MANET using symmetric and asymmetric cryptography.” Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2015 4th International Conference on. IEEE, 2015

[2]. Pushpalatha, K.; Chitra, M.,"GAMANET: A ganatic algorithm approach for hierarchical group key management in mobile adhoc network", IEEE,Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on,2013

[3]. Jun Zheng; Sanchun Xu; Fangfang Zhao; Dianxin Wang; Yuanjun Li,"A novel detective and self-organized certificateless key management scheme in mobile ad hoc networks", IEEE, Granular Computing (GrC), 2013 IEEE International Conference on,2013

[4]. Liu, Q.S.; Zhang, D.S.; Zhao, Y.,"Study on framework of distributed key Management for MANETs",IET,Information and Network Security (ICINS 2013), 2013 International Conference on,2013

[5]. Qianhong Wu; Bo Qin; Lei Zhang; Domingo-Ferrer, J.; Manjo; n, J.A.,"Fast transmission to remote cooperative groups: A new key management paradigm",IEEE,Networking, IEEE/ACM Transactions on,2013

[6]. Kodali, R.K.; Chougule, S.; Agarwal, A.,"Key management technique for heterogeneous wireless sensor networks",IEEE,TENCON Spring Conference, 2013 IEEE,2013

[7]. Xie Hai-tao,"A Cluster-Based Key Management Scheme for MANET",IEEE,Intelligent Systems and Applications (ISA), 2011 3rd International Workshop on,2011.

[8]. Bala Krishna, M.; Doja, M.N.,"Symmetric key management and distribution techniques in wireless ad hoc networks",IEEE,Computational Intelligence and Communication Networks (CICN), 2011 International Conference on,2011

[9]. Zhang Chuanrong; Liu Weijiang,"New ID-Based Signcryption Scheme and Its Applications in Key Update Protocols of MANET",IEEE,Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2010 International Conference on,2010

[10]. Yonglin Ren; Boukerche, A.; Mokdad, L.,"A novel framework of secure network management for wireless and mobile networks",IEEE,Local Computer Networks (LCN), 2010 IEEE 35th Conference on,2010

[11]. Nguyen, D.T.; Soh, B.,"Key Management for Lightweight Ad-hoc Routing Authentication",IEEE,Wireless Pervasive Computing, 2009. ISWPC 2009. 4th International Symposium on,2009

[12]. Luo Junhai,Ye danxia,Xue Liu& Fan Mingyu," Suvey of Multicast Routing Protocols for Mobile Adhoc Networks, Vol 11(1).2009

[13]. Boukerche, A.; Yonglin Ren,"The design of a secure key management system for mobile ad hoc networks",IEEE,Local Computer Networks, 2008. LCN 2008. 33rd IEEE Conference on,2008

[14]. Chadha, R.; Kant, L.,"Configuration Management",Wiley-IEEE Press,Policy-Driven Mobile Ad hoc Network Management,2008

[15]. Aurisch, T.; Ginzler, T.; Martini, P.,"Practical efficiency analysis of a dual mode group key management",IEEE,Military Communications Conference, 2008. MILCOM 2008.

[16]. Boukerche, A.; Yonglin Ren; Samarah, S.,"A Secure Key Management Scheme for Wireless and Mobile Ad Hoc Networks Using Frequency-Based Approach: Proof and Correctness",IEEE,Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE,2008

[17]. Hegland, A.M.; Winjum, E.; Mjolsnes, S.F.; Rong, C.; Kure, O.; Spilling, P.,"A survey of key management in ad hoc networks",IEEE,Communications Surveys & Tutorials, IEEE,2006

[18]. Young-Sik Hwang; Seung-Wan Han; Taek-Yong Nam,"The expansion of key infection model for dynamic sensor network", IEEE,Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference,2006