International Journal of Research in Advent Technology, Special Issue, March 2019
E-ISSN: 2321-9637
International Conference on Technological Emerging Challenges (ICTEC-2019)
Available online at www.ijrat.org

Detection of Malicious Link Using a Novel Routing Technique

G. Venu Gopal Rao[1] , D. Anand Rao[2]
[1]*Associate Professor, Department of MCA, JKC College, Guntur, Andhra Pradesh*
[2] *Assistant Professor, Department of CSE, Vikas Group of Colleges, Vijayawada, Andhra Pradesh.*
[1] *v_gudivada@yahoo.com* , [2] *desaraju.anand@gmail.com*

Abstract: The custom of communication security protocols initially advanced for wire line and Wi-Fi networks is present heavy burden on the limited network resources of a MANET. We propose new authenticating nodes is communication network on the basis of concept of shared trust. The propose algorithm is find secures and shortest path against wormhole attack. Routing mobile ad-hoc network is challenging dynamic topologies. There is lots of trust models and routing protocol which are used in MANETs security. An adaptive probing technique detects a malicious link through binary search and according to the nodes behavior these links are avoided in the active path by multiplicatively increasing their weights. Among these the security is the peak issue faced by most of the wireless networks. The research work proposes a framework that detects the selective forwarding attacks and computes the harmful hosts residing an ad-hoc structure. Simulation studies are conducted using NS2 to prove that proposed approach enhance network performance when network size, load or the mobility increases.
Index Terms: security, wormhole, shortest path, Mobile ad-hoc networks, applications, attacks, secur, Binary Search Probing, Reliability

1. INTRODUCTION

Ad-hoc network is considered as one of the most emerging technologies in today's world. In an ad-hoc network, the hosts rely upon one another to enable and maintain the entire network communicating and linked together [1]. The protocol safeguards pair wise communication across an unknown frequently changing network scheme presented in this paper guarantee that a byzantine fault is identified and the fault link can be avoided in the data transmission phase [2]. Various attacks can be reduced due to the presence of security protocols [3]. Different protocols are then evaluated based on packet drop rate, overhead introduced by routing protocol security issue faced by the routing protocol is taken into consideration [4]. Proactive approaches such as cryptography and authentication and many other techniques is proposed and implemented these applications are not sufficient. This can leave MANETs open to a range of attacks such as the Sybil attack and route guidance attacks that can conciliate the integrity of the network [5]. The work reported in this paper address the routing issues of accessible routing protocol in environment of MANETs and the routing recital in challenging environment of MANETs [6].

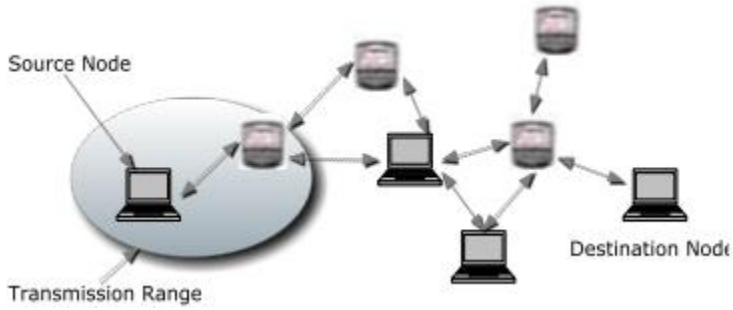

Fig. 1 Mobile Ad-hoc Network

2. RELATED WORK

Since the advent of MANETs, design and implementation of an efficient routing protocol with good performance and less overhead is one of the fundamental challenges of this network [7]. This paper is intended to aid researchers in developing their own on-demand ad hoc routing protocols and promoting users in influencing the employment design that best fits their needs [8]. The different aspects of proposing security models in MANETs to

relate to trust can be seen in information technology as trust metrics and trust evaluation are mainly defined for public key authentication to access control and electronic commerce [9].Hierarchical routing and geographic position assisted routing the increase in scalability can be achieved by reducing the number of rebroadcasting nodes [10]. In some times we need to keep the information secret from all of the unauthorized node or because of this may be malicious nodes and can interrupt or destroy the information. So we have to maintain the confidential information from the unauthorized entity [11]. The message and the redundancy are divided into a number of pieces, so that even a partial reception is able to reconstruct the data called as Message dispersion source updates the ratings of the paths based on the feedback [12]. The secure key management scheme was based on the threshold cryptography scheme worked efficiently when it had to deploy in large scattered areas. The mobiles nodes contact the servers. A refreshing scheme was used to counter the mobile node adversaries [13].

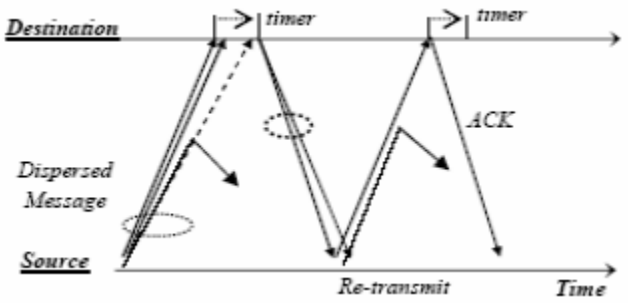

Figure 2. Message Dispersion in SMT

3. SYSTEM ARCHITECTURE

The hybrid routing protocol is characteristics of both reactive and proactive routing protocols is introduced the overheads ratio and the initial route discovery delays of existing routing protocols [14]. These internal attacks sometimes may broadcast wrong type of routing information to other nodes internal attacks are malicious nodes that are part of the network, internal attacks are more difficult to detect than the external attacks [15]. Signal Stability Based Adaptive (SSA) and Associatively-Based Routing (ABR) protocols propose two different mechanisms for assessing link stability. To avoid such cases the decision factor uses a global dynamic threshold value for guarantee the node to stay in the communication otherwise leave the network [16]. The new proposed method is backbone routing path is overhead and consume more bandwidth and nodes power in communication different terrains pose separate challenges to routing in high dynamic environment of MANETs [17].

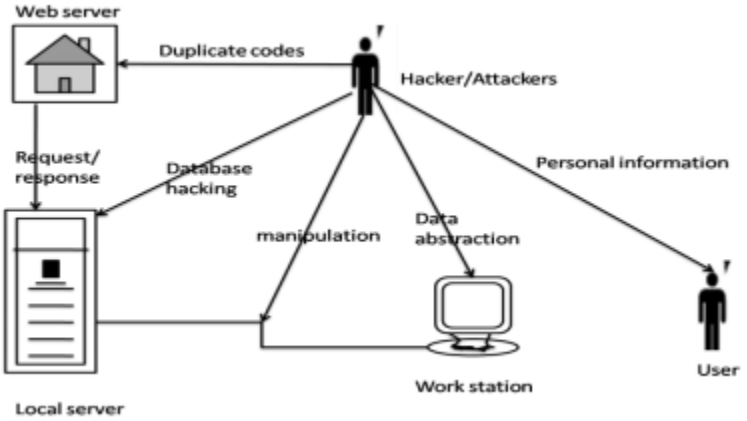

Fig No 3. Short Path Receiver

4. PROPOSED SCHEME

The security data transmission is increased selecting most secured routes in Active Path Set (APS) to improve the performance of the secured message transmission most reliable paths is selected and included in active path set APS is mechanisms is provided select the most reliable paths [18]. The route request is forwarded hop by hop and digital signatures are used at each hop to prevent an adversary from specifying an arbitrary path route discovery phase consists of the following phases [19].

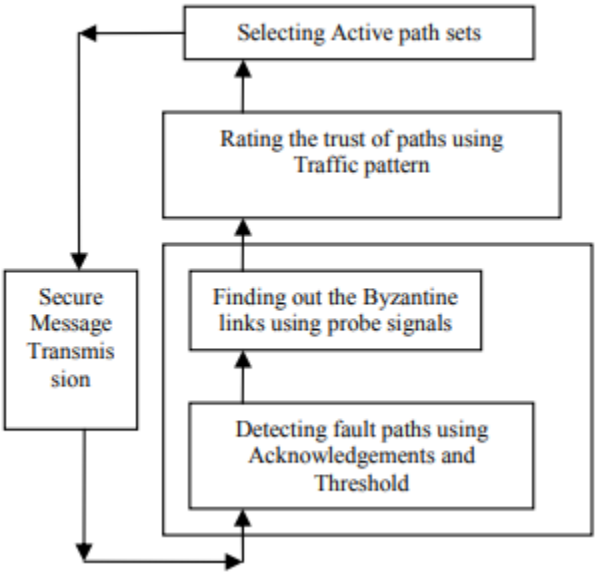

Figure 4. Overall view of proposed system

5. SECURITY ALGORITHM

The area is small the nodes assumed to be less malicious activity created by the wormhole attack will be monitored and the malicious node will be isolated the idea of shortest path algorithm is probabilistic method of analysis will be studied to cryptographic analysis will be made to run in a real time environment using a real time operating system. The hash chain is implemented on each packet to make the communication secure. The control packet is sent with each data packet [20]. There are three cases of control ACK; a) positive control ACK, b) negative control ACK and, c) no control ACK c Control ACK" presents the three cases of control ACK.

Algorithm: Retrieve hash field value algorithm

Step1: If (Final – Hash = F Hop Count (Hash)) then

S**tep2**: Retrieve the packet count value in the Hash field of the control packet

Step3: else

Step4: Drop the control packet

Key Management

We are taking multi-nodes in our system each host has manifold paths to reach a single terminus node in the network. The Daffier-Hellman key-exchange procedure offers a means of making symmetric key generation possible and is cast off to make the Symmetric Keys (SK) keys. Symmetric Broadcast keys (SKb) can only be produced by means of an algorithm that generates random number of corresponding protected key generation service [21]. This is accomplished using a hashing algorithm such as HMAC. Thus the packet's journey from point-to-point until the destination is reached is pragmatic [22].

INPUT: NODES, TA, PUBKEY, PRIKEY

STEP1: Node is provided with a certificate from a TA

STEP2: The joining node A seeks to join a network by periodically broadcasting Discovery Request packets containing its Public Diffie-Hellmen Key Share (DKSp). This continues until it receives a Certificate Request from a networkable node B.

STEP3: A sends its certificate in a Certificate Exchange packet to B.

STEP4: B checks the integrity and authenticity of the Certificate Exchange (CEx)packet, using the shared SKp.

STEP5: If the certificate is deemed authentic A is added to B's security table. If the certificate fails this

check, the DKSp, SKe and SKp credentials generated for node A by B is dropped and B and the process ends.

STEP6: If B has not yet authenticated any other nodes, it will generate an SKb, prior to sending it to the joining node otherwise it will send the current SKb to the joining node.

STEP7: If A has a broadcast key, it transmits a Broadcast Key Exchange (BEx) packet containing the new key, secured with the original key before committing the new key to its security table.

STEP8: B broadcasts an SK Invalidation (SKI) packet, invalidating any previous credentials A may have had with nodes within the network.

6. EXPERIMENTAL RESULTS

The experiments substantiate that the proposed system is successfully cope with a high number of adversaries, Active Path Set Secure Message Transmission is deliver many packets successfully than Non-Secure Protocol is successful end to-end delay. Network throughput is decreased as there is a presence of malicious nodes in malicious node interrupts with the communication held between the nodes of the network the throughput of the network drops. the malicious nodes, their packets are no longer floating in the network plus there is also no need to resend the dropped packet hence increasing the overall performance and reducing the overhead of the network. The network coverage is a 500m by 500m with 50 mobile nodes, with any two nodes able to communicate if they are within the reception distance which is set to 150m.

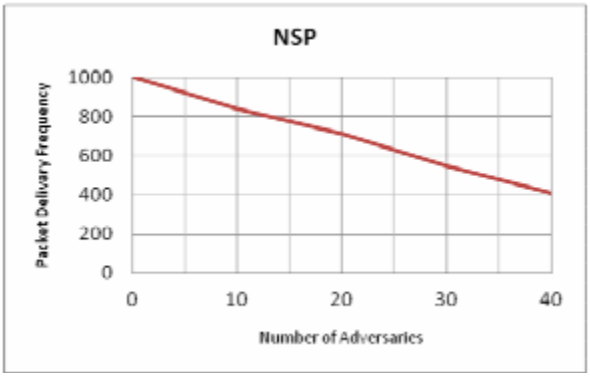

Figure 5. Performance of NSP

7. CONCLUSION AND FUTURE WORK

The work is formulated to an advanced mathematical concept to extend to a Wide area Network. Our proposal is distributed effective and does not depend itself on any central network to direct interaction among nodes in the network is taken into account as a quantity of experience. These are classified as active and passive attacks is try to implement security algorithm along with routing protocols which help to reduce the effect of different attacks. The successful delivery of message with the ability to disperse and avoidance of faulty links is more reliable than ordinary secured data transmission mechanism. We developed and simulated a framework for the detection of selective forwarding attacks using MANET technologies. A network environment is deployed and several experiments were performed for the verification and validation of the proposed solution. Future work is direction to trim down the ratio of End to End delays is enhance the recitation of the network new way.

REFERENCES

[1] C.-Y. Chong and S. Kumar, “Sensor networks: Evolution, opportunities, and challenges,” Proc. IEEE, vol. 91, no. 8, pp. 1247–1256, Aug. 2003.

[2] MENG Limin, SONG Wenbo* “Routing Protocol Based on Grover’s Searching Algorithm for Mobile Ad-hoc Networks” Network Technology And Application, China Communications • March 2013

[3] Israat Tanzeena Haque “On the Overheads of Ad Hoc Routing Schemes” IEEE Systems Journal, 2013.

[4] Wei-Liang Shen, Chung-Shiuan Chen “Autonomous Mobile Mesh Networks” IEEE Transactions On Mobile Computing, Vol. 13, No. 2, February 2014.

[5] Wei Liu and Ming Yu “AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments” IEEE Transactions On Vehicular Technology, Vol. 63, No. 9, November 2014.

[6] B. Ramakrishnan, Dr. R. S. Rajesh, R. S. Shaji "CBVANET: A Cluster Based Vehicular Adhoc Network Model for Simple Highway Communication"
[7] M. Hyland, B. E. Mullins, R. O. Baldwin, and M. A. Temple, "Simulation-based performance evaluation of mobile ad hoc routing protocols in a swarm of unmanned aerial vehicles," in Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 249–256.
[8]J. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, "Performance analysis of mesh routing protocols for uav swarming applications," in Wireless Communication Systems (ISWCS), 2011 8th International Symposium on. IEEE, 2011, pp. 317–321.
[9]H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," Wireless Communications, IEEE, vol. 11, no. 1, pp. 38– 47, 2004.
[10]N. Garg and R. Mahapatra, "Manet security issues," IJCSNS, vol. 9, no. 8, p. 241, 2009.
[11] Herzberg, A., Y. Mass, and J. Michaeli. Access control meets public key infrastructure, or: assigning roles to strangers. in Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. 2000. Berkeley, CA, USA: IEEE.
[12] D. Johnson, D. Maltz and J. Broch., "DSR The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks", chapter 5, Addison-Wesley, 2001. Pages 139–172.
[13] A.B. McDonald, T.F. Znati. "A mobility-based framework for adaptive clustering in wireless ad hoc networks, "IEEE Journal on Selected Areas in Communications, vol. 17, No 8, Aug. 1999.
[14] R. Dube, C.D. Rais, K.Y. Wang, and S.K. Tripathi, "Signal Stability-Based Adaptive Routing (SSA) for Ad Hoc Mobile Networks", IEEE Personal Communications, p.36-45, Feb. 1997.
[15] C.K. Toh "Associativity-Based Routing for Ad Hoc Mobile Networks" International Journal on Wireless Personal Communications, Vol. 4, No. 2, 1997.
[16] R.L. Rivest, A. Shamir, and L. Adleman "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge. [17] W. Diffee and M. E. Hellman "New directions in cryptography". IEEE Transon Information Theory IT22(6):644-654, November 1976.
[18] N. H. Mistry1, D. C. Jinwala2 and M. A. Zaver, "MOSAODV: Solution to Secure AODV against Blackhole Attack", International Journal of Computer and Network Security, Vol. 1, No. 3, December 2009 pp:42-45.
[19] M. P. Shelke, A. Malhotra and P. Mahalle, "A packet priority intimation-based data transmission for congestion free traffic management in wireless sensor networks," Computers & Electrical Engineering, vol. 64, pp. 248-261, 2017.
[20] V. K. Saurabh, R. Sharma, R. Itare and U. Singh, "Cluster-based technique for detection and prevention of black-hole attack in MANETs," in International conference of Electronics, Communication and Aerospace Technology (ICECA), 2017.
[21] L. Baghel, P. Mishra, M. Samvatsar and U. Singh, "Detection of black hole attack in mobile ad hoc network using adaptive approach," in Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of, 2017.
[22] D. Gayathri and S. J. Raman, "Pltrust AODV: Physical logical factor estimated trust embedded AODV for optimised routing in Manets," in Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on, 2017.