A HYBRID KEY MANAGEMENT SCHEME FOR SECURE MANET COMMUNICATIONS

A.Pranusha[1], G. Murali[2]

[1]*M. Tech, Computer Science and Engineering, JNTUA College of Engineering, pulivendula, Andhra Pradesh, India*
[2]*Assistant professor of Computer Science and Engineering, JNTUA College of Engineering, Pulivendula Andhra Pradesh, India*

Abstract

In MANETs communication is done using a shared wireless channel. There is no provision for monitoring authority. The nodes in the network need to take the responsibility for both data transfer and also security. For robust security in MANETs, key management scheme is essential. However, secure key management is a challenging problem to be addressed. In this paper, we focused on a hybrid technique that makes use of identity and trust which enables to identify malicious nodes and also convert malicious node into a trusted node. Our hash technique is evaluated with NS2 simulations. The results reveal that the proposed system is able to identify malicious nodes in MANET and handle malicious nodes in such a way that they become trusted nodes.

Keywords *– Mobile Ad Hoc Network, trust model, malicious node detection, security*

----------***----------

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) is the network with multiple nodes that do not need fixed infrastructure. They are configured automatically and they are used to have effective and cost effective communications. MANET has become an attractive solution that can be used in various applications in the real world. The nodes in the MANET can act as both transmitter and receiver. The nodes will transmit packets of other nodes in order to send them to intended destination.

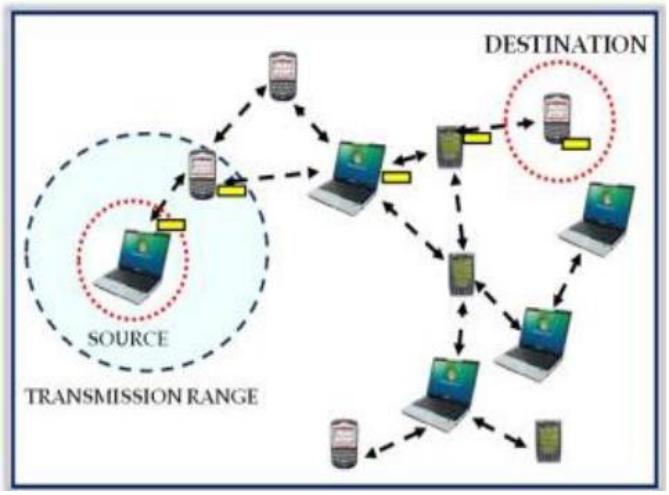

Fig 1 – Illustrates a MANET [18]

As can be seen in Figure 1, it is evident that the MANET nodes are self configured without having fixed infrastructure. In this paper we proposed a new scheme to secure communications in MANET. However, our work in this paper in confined to the identification of malicious nodes and applying trust factor to them in order to ensure that every node in the MANET becomes trustworthy and genuine. The remainder of the paper is structured as follows. Section 2 presents review of literature. Section 3 presents the proposed system. Section 4 shows simulations and results while section 5 provides conclusions and directions for future work.

2. RELATED WORK

This section provides review of related works pertaining to key management systems in MANET. Gowthami and Bhuvaneswari [1] proposed a trust based and attributed scheme for secure authentication mechanism in MAENT. This scheme reduces complexity in key distribution. Rajeswari and Priya [2] proposed an optimal key management scheme for MANET. Their security architecture combines both grid architecture and key management. Chahal et al. [3] made a review of secure key management schemes in MANET. Similar kind of work is done in [6], [12]. Saha et al. [4] present different key management schemes that could prevent various attacks. Kaushik and Singhai [5] applied reputation based scheme for identifying reluctant nodes in MANET.

YI and Nantes [7] discuss the security issues in MANET. Memon et al. [8] proposed a framework for QoS management. Xiong and Tang [9] proposed a key management scheme to MANET which is very secure and efficient. Yvuz et al. [10] applied syncryption and hybrid cryptography for MANET used in military. Sudarsan et al. [11] proposed a new intrusion detection scheme for MANET. Anand and Vedhavarshini [13] proposed a hybrid scheme that is meant for securing communications in MANETs. Sighoml and Raciti [14] focused on data leakage prevention in MANET using best-effort approach. Abushag and Deepalakshmi [15] worked on the secure group communications in MANET without relying on a trusted third party. Schuttle [16] presented a scheme that detects

malicious and selfish nodes in MANET. Zamani and Zubair [17] discussed about many key management solutions for MANET. In this paper we proposed a novel hash based scheme for detecting malicious nodes and applying trust factor to them to make them trustworthy.

3. PROPOSED SYSTEM

The aim of the proposed system to use trust factor and identity based security in order to have robust communications in MANET. The trust factor is considered when a node is selected in MANET for communications. We implemented a hash based technique to ensure that the nodes are authenticated correctly. The authentication prevents malicious access to the network. Moreover the proposed scheme makes use of hybrid approach in which when one flavor of security is compromised other portion of security can still protect MANETs to have secure communications. The nodes in the network generate key value pairs and they are periodically updated. The trust factor on the nodes indicate that the genuine behavior of nodes. The nodes that transmit packets correctly will have good trust factor while the nodes that do not involve in other nodes' packet transmission, they are said to have misbehaved and their trust value gets affected.

4. SIMULATIONS AND RESULTS

The following table shows the simulation parameters and descriptions.

PARAMETER	SPECIFICATION
Simulation tools used	NS2 Network Simulator (ns-2.35)
Simulation time	60 sec, 120 sec, 200 sec
Number of nodes	30
Transmission range	250m
Maximum speed	0-20 m/sec
Application traffic	CBR [constant bit rate] [20]
Packet size	512bytes
Node mobility model	10 packets/sec
Routing Protocol	AODV

With these parameters, simulations are made in NS2. The performance level of proposed scheme was evaluated just before the trust factor is applied and after trust factor is applied. The results are presented in Figure 2 and Figure 3.

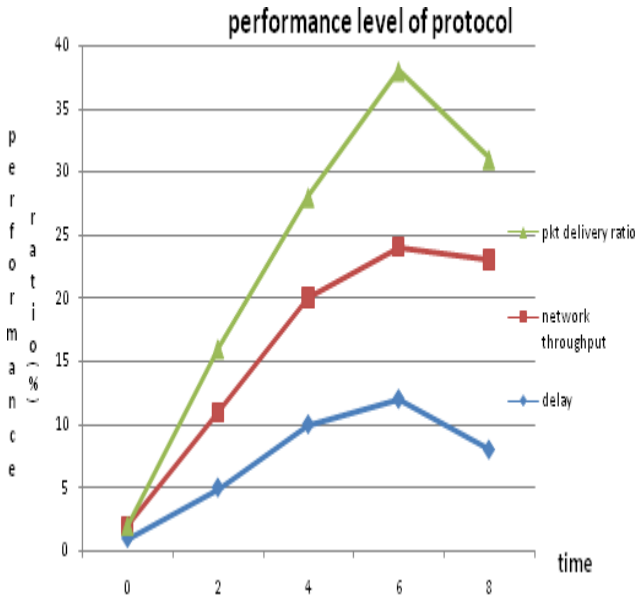

Fig 2 – Performance of protocol before applying the trust factor.

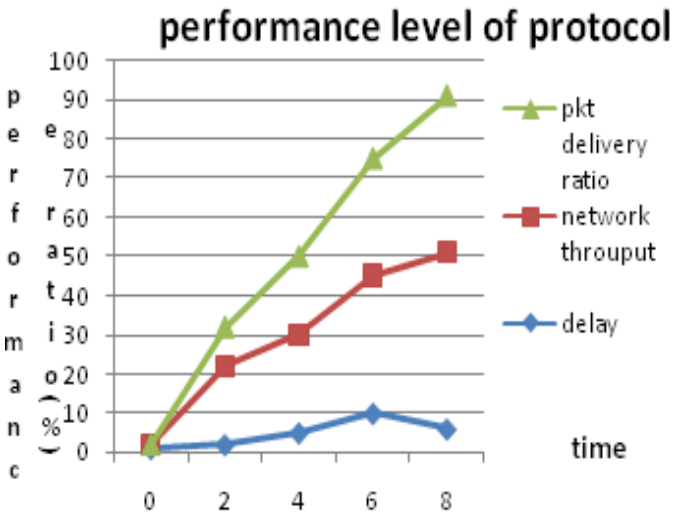

Fig 3 – Performance of protocol after applying the trust factor.

As can be seen in Figure 2, the results reveal the simulation dynamics with respect to packet delivery ratio, network throughput and delay performance. The horizontal axis represents time while the vertical axis represents performance ratio. Performance level of protocol is less before applying the trust factor.

After applying trust factor the performance level of protocol is improved in terms of packet delivery ratio, network throughput and delay performance. It is shown in figure 3.

5. CONCLUSION AND FUTURE WORK

In this paper we studied MANET security issues and implemented a scheme based on hash that could protect MANET communications. Our work in this paper is confined to finding malicious nodes and applying them trust factor in such a way that they are handled well and they

become trusted nodes. The proposed technique will ensure that every node in the network is trustworthy and has integrity with other nodes in working with protocol compliance and its responsibilities towards transferring packets. Thus the network performance improved in terms of packet delivery ratio, throughput and other aspects. In future this research will be extended further with a more comprehensive scheme that provides fool proof security in MANET communications.

REFERENCES

[1]. V.Gowthami1, R. Buvaneswari2 (2013). An Efficient Attribute Based Schema for Trust and Cluster Based Authentication Mechanism in MANET. ISSN. 2 (6), p2320 - 2602.

[2]. S. Rajarajeswari (2013). An Optimal key Management for MANE .ISSN. 2 (1), p2319 – 1058.

[3]. Anju Chahal1 and Anuj Kumar2, Auradha2. (2014). SECURE KEY MANAGEMENT IN AD-HOC NETWORK: A REVIEW. Issn . 7 (3), p1009-1017.

[4]. Himadri Nath Saha, Dr. Debika Bhattacharyya , Dr. P. K.Banerjee Aniruddha Bhattacharyya ,Arnab Banerjee , Dipayan Bose . (2012). STUDY OF DIFFERENT ATTACKS IN MANET WITH ITS DETECTION&MITIGATION SCHEMES. International Journal of Advanced Engineering Technology. 3 (1), p0976-3945.

[5]. Rekha kaushik and Jyoti Singhai. (2011). DETECTION AND ISOLATION OF RELUCTANT NODES USING REPUTATION BASED SCHEME IN AN AD-HOC NETWORK. International Journal of Computer Networks & Communications. 3 (2), p95-105.

[6]. Bing Wu. (1996). A Survey of Key Management in Mobile Ad Hoc Networks. Bing Wu, p1-16.

[7]. Jiazi YI, Polytech'Nantes (2008). A NOTE ON THE SECURITY OF MANETS .MANET, p1-23.

[8]. M. Sulleman Memon, Manzoor Hashmani and Niaz A. Memon. (2009). A Framework for QoS Management and Contract Enforced Services in MANETs for Prioritized Traffic Environment. IJCSNS International Journal of Computer Science and Network Security. 9 (4), p192-198.

[9]. Wan An Xiong, Bin Tang. (2011). A Secure and Highly Efficient Key Management Scheme for MANET. A Secure and Highly Efficient Key Management Scheme for MANET. 3 (2), p12-22.

[10]. Attila A. YAVUZ1, Fatih ALAGOZ2, Emin ANARIM3. (2010). A new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption. T¨UB˙ITAK. 18 (1), p1-21.

[11]. Ms Shyama Sudarsan, Mrs Vinodhini, Dr S.Karthik. (2012). Enhancing Key Management In Intrusion Detection System For Manets. ISSN. 1 (8), p2278 – 1323.

[12]. Deepak Chopra Shaila Chugh Deepak Sain. (2013). Survey of Secure Communication Techniques in Mobile Ad-hoc Network. ISSN . 2 (3), p2319-2720.

[13]. Anand .T , Vedhavarshini .R. (2013). Secure Hybrid Key Scheme to Detect Malicious Nodes in Manets. ISSN. 3 (6), p2013-2016.

[14]. Johan Sigholm. (2012). Best-Effort Data Leakage Prevention in Inter-Organizational Tactical MANETs. Department of Computer Science, p1-16.

[15]. S.Fiona abishag, Dr.P.Deepalakshmi. (2014). Secure group communication over MANET using hybrid Key Management.International Journal of Scientific & Engineering Research. 5 (5), p690-694.

[16]. Martin Schütte. (2006). Detecting Selfish and Malicious Nodes in MANETs. SICHERHEIT IN SELBSTORGANISIERENDEN NETZEN, p1-16.

[17]. Ad Hoc Networks Abu Taha Zamani, Syed Zubair. (2014). Key Management scheme in Mobile Ad Hoc Networks. ISSN. 3 (4), p2278-9359 .

[18] Sensors, Available online at http://www.mdpi.com/1424-8220/11/4/3652 [Accessed: 10 March 2015]