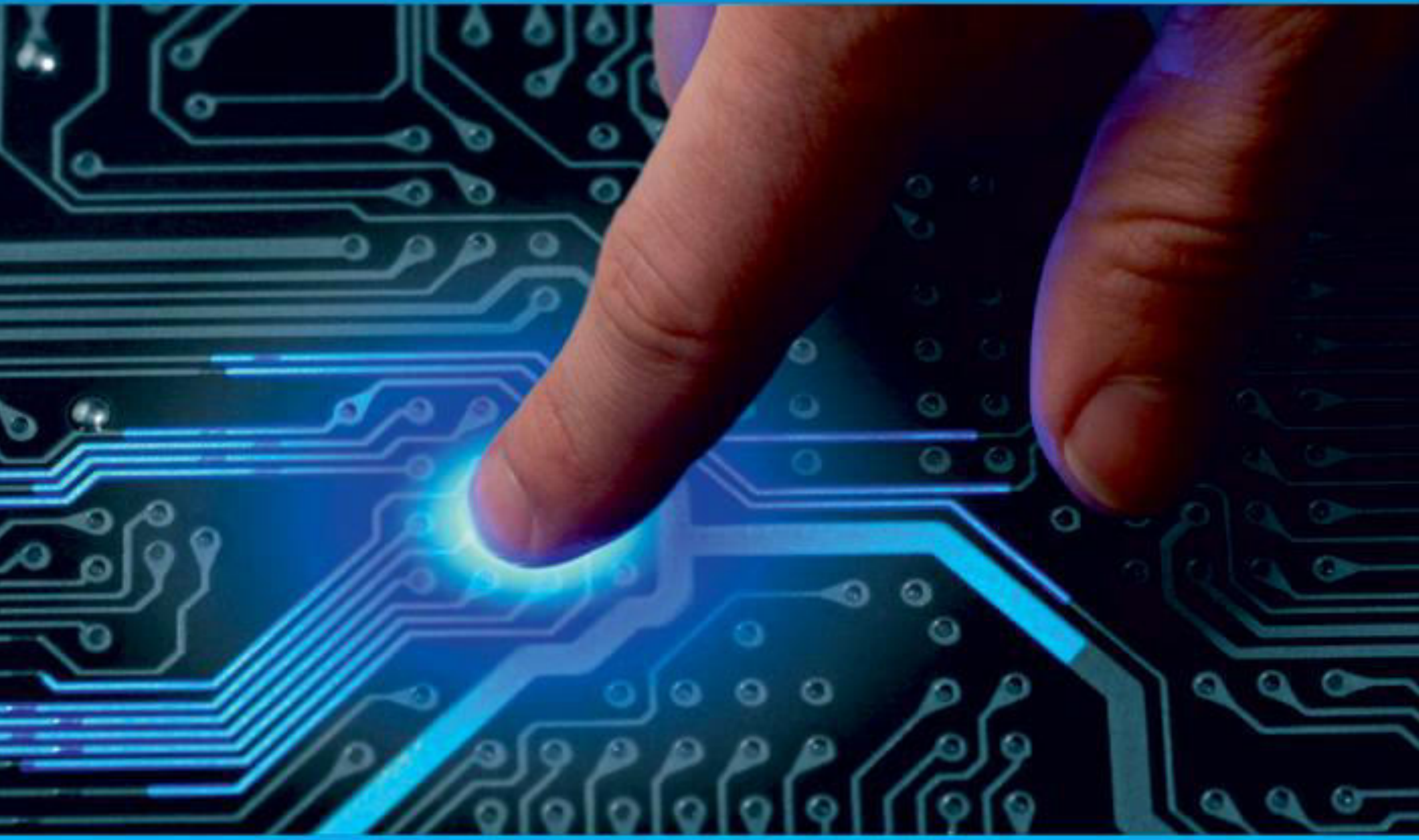
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 11, November 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

| DOI: 10.15680/IJIRCCE.2021.0911009 |

Review on Integrated Localized Key Management Protocol with Efficient Secure Routing in MANETs

Swapnali Swami, Kiran Khandarkar

Post Graduate Student, Dept. of Computer Science and Engineering, Maharashtra Institute of Technology (MIT), Aurangabad, Maharashtra, India

Dept. of Computer Science and Engineering, Maharashtra Institute of Technology (MIT), Aurangabad, Maharashtra, India

ABSTRACT: Mobile ad hoc network (MANET) is a self-configuring and multi hopwireless network. It is more vulnerable to different types of attacks and securitythreats because of its characteristics and network is not secure due to the mobilityand dynamic nature of mobile ad hoc network. A routing protocol in a mobile ad hoc network should be protected against both inside and outside attackers. Most of the routing protocols in MANET assume that all the nodes in a network will cooperateto each other while forwarding data packets to other nodes. But intermediatenodes may cause several problems like it can deny in packet forwarding, also can extractuseful information from the packet or may modify the content of packet.Such nodes are known as misbehaving nodes. The efficient key managementprotocol can address these issues in MANET by applying suitable cryptographyor encryption techniques which can prevent attackers. In MANET on demandrouting protocols provide cost effective and scalable solutions for packet routingbut the path generated by these protocols may deviate far from the optimalpath because of the lack of knowledge about the global topology and the mobilityof nodes. Routing optimality also affects network performance and energyconsumption. So here by using Efficient Secure Routing Localized KeyManagement (ESR-LKM) protocol we can optimize the path dynamically to increase performance and reduce energy consumption. The proposed path awareESR-LKM algorithm finds the shortest path by reducing the number of hops. Andto prevent attackers efficient key management and cryptography is used.

KEYWORDS: Mobile ad hoc network, Misbehaving nodes, Secure routing, Keymanagement.

I. INTRODUCTION

Mobile ad hoc network (MANET) is a typical multi-hop wireless network that composedof several mobile nodes with computing and communication capabilities. Each node of MANET act as a sender, receiver and in some cases as a router as well. InMANET intermediate nodes may cause several problems like it can drop useful packets, can deny to packet forwarding or may modify the contents of packets during the datatransmission session. Such nodes are referred as misbehaving or malicious nodes. Thiscan be prevented by authenticating all routing control packets so that outside attackerscannot participate in the route discovery process. In MANETs nodes are easy tocapture and hence a malicious node which holds valid keys cannot be prevented fromparticipating in the route discovery process. So such inside attackers can be preventedby using intrusion detection system [8].

Major challenges for routing in MANETs are low transmission power, dynamic topology i.e. continuouslychanging network topology and low bandwidth. With the increase in the size and averageroute length, scalability becomes an issue for the current ad hoc routing protocols.Table-driven proactive routing protocols that require periodic advertisement and globaldistribution of information are not suitable for large networks like MANETs. For routingin large ad hoc networks, on-demand routing protocols [6], [9] i.e. reactive or dynamic routingprotocols are efficient because they maintain the routes as per need byinitiating the path discovery process.

The goal of this work is to optimize the path dynamically between the source and destination, to enhance the performance and reduce energy consumption as well asproviding security against attackers.

| DOI: 10.15680/IJIRCCE.2021.0911009 |

II. RELATED WORK

The SR-LKM protocol [1] uses a localized key management mechanism and in thisa network node performs all key management activities within its one hop neighborhoodonly. This protocol is free from key management secure routing interdependencyproblem because the localized key management approach used in this protocol is independenton any secure routing protocol. For broadcast key distribution, it uses the LCMbased broadcast key distribution mechanism. It can prevent both inside and outside attackerswith the help of a monitoring based revocation mechanism. Its per node storagerequirement is not dependent on the total number of nodes in the network so it is storagescalable. The drawback of this protocol is that it assumes an offline CA existing outsidethe network which distributes the PKCs to all the nodes in the network. But if the CAis not trusted then the network is not secure.

The SELRAN [2] uses digital signatures to ensure the authentication and the integrityof the routing messages and prevent internal attacks such as malicious alteration.It uses secure link state update procedure and secure neighbor establishment procedureto detect internal attacks. Secure and efficient proactive topology is also provided bythis protocol. The drawback of this protocol is that the digital signatures used to authenticatethe routing messages are expensive and the colluding attacks such as wormholeattacks cannot be detected by this protocol.

SLSP [3] provides secure proactive topology discovery. It is robust against individualattackers and can adjust its scope between local and network-wide topology discovery.It is capable of operating in networks of frequently changing topology andmembership. The drawback of this protocol isthat it only concerned with securing thetopology discovery and does not guarantee that adversaries complied with its operationduring the route discovery would not attempt to disrupt the actual data transmissionlater.

SRDP [4] uses aggregated MACs or multi-signatures to securely discover an authenticatedroute from the source to the destination. Aggregation allows compressingauthentication tags hence saves bandwidth and reduces verification costs. To authenticatethe route, it uses forward and backward authentication. The drawback of thisprotocol is that the source node has to verify all MACs attached with a RREP messageproduced by the intermediate nodes so verification cost at the source node increaseswith the route length.

KM SR [5] uses IBC for establishing the symmetric keys and authenticating therouting messages and provides security features such as authentication, confidentiality,freshness and non-repudiation. It is secure because it uses 1-to-m broadcast keyinstead of only one group broadcast key and has less keys to store per node. It hasno KM-SR interdependency cycle problem and due to IBC properties the storage andcommunication requirements are lower as compared to PKI. It is secure from inside attacks,mobile attacks and many routing attacks. The drawback of this protocol is that ituses computationally expensive digital signatures to authenticate the routing messagesand it consumes more energy due to its IBC operations so it is not suitable for resourceconstraint MANETs.

SE- AODV [6] uses symmetric key cryptography for authenticating routing controlpackets. SE- AODV adds extra features to same AODV routing protocol and makespath formation more secure. In this a GTK encrypted with PTKs is distributed by eachnode to all of its neighbors, so such key bandwidth mechanism is highly bandwidthconsuming.

In an Efficient Authentication and Signing of Multicast Streams over Lossy Channels[7], two efficient schemes TESLA and EMSS are proposed. TESLA offers senderauthentication, strong loss robustness, high scalability and minimal overhead at the cost of loose initial time synchronization and slightly delayed authentication. EMSS providesnon-repudiation of origin, high loss resistance and low overhead at the cost ofslightly delayed verification. In this a node authenticates the RREQ packets using hashchainbased TESLA keys. But a TESLA key is disclosed after a certain amount of delayso each node needs to buffer the control packets in its memory until the sender disclosesthe TESLA key. So it leads to a higher storage overhead and delayed packet delivery.

In On Intrusion Detection and Response for MANET [8] they presented networkintrusion detection mechanism that is used to detect misbehaving nodes in MANET.They presented two response mechanisms which are active and passive. In passiveresponse if a node finds any intrusive node then it raises an alarm and removes thatintrusive node from its neighbor table and will no longer participate in route discoveryprocess with that node. In active response when a node raises an alarm, then it forwardsthat alarm to its entire cluster heads. After that cluster head initiates a voting processand if the majority determines that the suspected node is intrusive then an alert will bebroadcast throughout the network. The drawback of this intrusion detection mechanismis that a misroute cannot be determined in this and if most of the cluster heads aremalicious nodes then the voting scheme can fail.

| DOI: 10.15680/IJIRCCE.2021.0911009 |

III. PROBLEM DEFINATION AND OBJECTIVE

A MANET is a collection of independent mobile nodes with self-configuring and self-administratingfeatures. In MANET initial work for routing was done addressing thepath formation between nodes. In such a network any node can join and leave thenetwork. Routing protocol addressed for only efficient path formation makes the samenetwork vulnerable to various attacks. Packets that are routed during route discoveryprocess need to be protected in such a way that it has a least probability of having amalicious node in path formed.
Ill formed paths longer than the shortest available paths are also not desirable becauseextra bandwidth is consumed and end-to-end delay is long. So it is necessary tooptimize the path dynamically between source and destination to enhance performanceand reduce energy consumption and to secure network against attackers.

The objective of this work is to develop integrated localized key management protocolin MANET which will optimize the path dynamically between source and destinationand will provide security against attackers. The objectives are stated as follows:
_ To provide a routing approach which is secure against both inside and outsideattackers.
_ To provide a routing approach which is promising in terms of energy efficiency as well as concerned with optimizing and hiding paths to reduce the number ofhops.
_ To provide a key management approach which is not dependent on any routingprotocol.

IV. CONCLUSION

MANET is a collection of independent nodes and these nodes can communicate witheach other via bidirectional links. The self-configuring ability of nodes in MANETmade it popular among various applications like in disaster recovery areas, in militaryuse, and communications in battle ground. Security, limited battery and performanceare the key issues in MANET. For MANET's communication a routing protocol is keyand it decides the performance of MANET. The proposed ESR- LKM can address theseissues in MANETs and can optimize the path dynamically to enhance performance andto reduce energy consumption. Unlike many of the existing authentication based securerouting protocols, the proposed protocol can prevent inside attackers also.

REFERENCES

[1]Shrikant H Talawar, SoumyadevMaity and R. C. Hansdah, “Secure Routing with anintegrated localized key management protocol in MANETs ”, IEEE 28th InternationalConference on Advanced Information Networking and Applications, pp. 605-612, 2014.
[2]L. Chen, J. Leneutre and J. J. Puig, “A secure and efficient link state routing protocolfor ad hoc networks”, In Proc. of the International Conference on Wireless and MobileCommunications, 2006.
[3]P. Papadimitratos and Z. J. Haas, “Secure routing for mobile ad hoc networks ”, In Proc.of the SCS Commnication Networks and Distributed Systems Modeling and SimulationConference, pp. 193-204, 2002.
[4]J. Kim and G. Tsudik, “Srdp: Secure route discovery for dynamic source routing inMANETs ”, In Proc of the Second Annual International Conference on Mobile and UbiquitousSystems: Networking and Services, 2005.
[5]S. Zhao, R. Kent and A. Aggarwal, “A key management and secure routing integratedframework for mobile ad-hoc networks ”, Tenth Annual International Conference onPrivacy, Security and Trust, pp. 96-103, 2012.
[6]Rajdeep S. Shaktawat, Dharm Singh and Naveen Choudhary, “An Efficient Secure RoutingProtocol in MANET Security-Enhanced AODV (SE-AODV)”, International Journalof Computer Applications, vol.97, no.8, pp. 34-41.
[7]A. Perrig, R. Canetti, D. Song and J. Tygar, “Efficient Authentication and Signing ofMulticast Streams over Lossy Channels”, In Proc. of the Network and Distributed SystemSecurity Symposium, vol. 1, pp. 35-46, 2001.
[8]J. Parker, J. Undercoffer, J. Pinkston and A. Joshi, “On intrusion detection and responsefor mobile ad hoc networks ”, In Proc. Of the IEEE International Conference on Performance,Computing and Communications, pp. 747-752, 2004.
[9]C. E. Perkins and E. M. Royer, “Ad-hoc On-Demand Distance Vector Routing”, In Proc.IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100, Feb. 1999.
[10]Zhou Yuan, Li Guangsheng, Mao Qirong, Zhan Yongzhao and HouYibin, “A DynamicBroadcast Ring Based Multicast Routing Protocol for Ad hoc Networks”, In Proc. of theInternational Conference on Computer Networks and Mobile Computing, 2003.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details