ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

A Review on Secure Routing Protocols in MANET

Komal Khedkar, Shubham Joshi

M.E. Student, Dept. of C.E., D.P.C.O.E. Wagholi, Pune, Maharashtra, India

Assistant Professor, Dept. of C.E., D.P.C.O.E. Wagholi, Pune, Maharashtra, India

ABSTRACT: Mobile Ad hoc network (MANET) is a collection of self configuring, multi-hop wireless network. Due to the mobility and dynamic nature of MANET, network is not secure. MANET is more vulnerable to different types of attacks and security threats because of its characteristics. A routing protocol in a mobile Ad hoc network should be secure against both inside and outside attackers. Most of the routing protocols in MANETs assume that all the nodes in a network will cooperate to each other while forwarding data packets to other nodes. But intermediate nodes may cause several problems like it can deny to forward the packet, can also extract useful information from the packet or may modify the content of packet. Such nodes are referred as malicious nodes. An Improvised Secure routing approach should be used to address these issues in MANET by applying suitable cryptography or encryption techniques which can prevent outside attackers. By applying intrusion detection system (IDS), internal attackers can be prevented. In this paper various previously used routing protocols are discussed. Analysis is done by considering various previously used mechanisms used by those protocols and aim is to find out one new authentication based approach for secure routing.

KEYWORDS: Mobile Ad hoc network (MANET), malicious nodes, Intrusion Detection System, Secure Routing, Key Management.

I. INTRODUCTION

Mobile Ad hoc network is a typical multi-hop wireless network that composed of several mobile nodes with computing and communication capabilities. Each node of MANET works as a sender as well as a receiver and sometimes as a router as well.

Most of the routing protocols in MANET assume that nodes in a network will cooperate to each other while forwarding data packets to another nodes. But intermediate nodes may cause several problems like it can extract useful information packets, can deny to forward packets or may modify the contents of packets during the data transmission session. Such nodes are referred as misbehaving nodes or malicious nodes. This can be prevented by authenticating all routing control packets using cryptography, so that the outside attackers cannot participate in the route discovery process.

Number of efficient routing protocols [2] – [9] are based upon the above strategy. Key management is essential to cryptography for key generation and distribution. But all these authentication based secure routing protocols need the support of an underlying key management mechanism to distribute the authentic keys among the nodes which exchange routing control packets among them.

An authentication based secure routing control protocols are dependent upon an underlying key management protocol. But in MANETs some existing key management protocols also depend on a secure routing for their functioning. This creates secure routing – key management cyclic interdependency problem. Hence, an authentication based secure routing protocol should use a key management mechanism which is not dependent on secure routing [2], [6], [8].

Nodes in a MANET are easy to capture and hence, a malicious node which holds valid keys cannot be prevented from participating in the route discovery process. So such inside attackers can be prevented by using intrusion detection system [10], [11].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

The goal of this work is to study different authentication based secure routing protocols and intrusion detection secure routing protocols in MANET with their advantages and pitfalls.

II. LITERATURE SURVEY

In MANETs secure routing protocols are basically of two types, A) authentication based protocols and B) intrusion detection system (IDS) based protocols. Authentication based protocols are mainly designed to prevent outside attackers and intrusion detection system based protocols are designed to prevent inside attackers.

The SR-LKM protocol [1] uses a localized key management mechanism and in this a network node performs all key management activities such as key establishment, renewal and revocation within its one hope neighborhood only. The localized key management approach used by this protocol is not dependent on any routing protocol. Hence, it is free from key management – secure routing interdependency problem. It uses a novel based handshaking and the LCM based broadcast key distribution mechanism which makes it lightweight. It can prevent both inside and outside attackers with the help of a monitoring based revocation mechanism. Its per node storage requirement is not dependent on the total number of nodes in the network, so it is storage scalable.

The SELRAN [2] uses digital signatures to ensure the authentication and the integrity of the routing messages and counter external attacks such as malicious alteration. But internal attacks cannot be countered by using pure cryptographic primitives. So more sophisticated Secure Link State Update Procedure (SLSUP) and Secure Neighbor Establishment Procedure (SNEP) was proposed to detect them. Counter-based mechanism was also used to reduce the broadcast overhead of the Link State Update packets (LSU) in this protocol which made it more efficient in resource-constraint environments such as ad hoc networks. The drawback of this protocol is, it uses computationally expensive digital signatures to authenticate the routing messages, and hence it is not suitable for resource constraint MANETs.

ARAN [3] uses public key cryptographic mechanisms to defeat all identified attacks. They also showed how ARAN can be secure in routing environments where nodes are authorized to participate but untrusted to cooperate, as well as environments where participants do not need to be authorized to participate. This protocol also uses computationally expensive digital signatures to authenticate the routing messages which is not suitable for resource constraint MANETs.

Panagiotis Papadimitratos and Zygmunt J. Haas have proposed SLSP [4] which provides secure proactive topology discovery. It can be employed as a stand-alone protocol or fit naturally into a hybrid routing framework, when combined with a reactive routing protocol. SLSP is robust against individual attackers, it is capable of adjusting its scope between local and network-wide topology discovery and it is capable of operating in networks of frequently changing topology and membership. The drawback of this protocol is that it is solely concerned with securing the topology discovery and it also does not guarantee that adversaries which complied with its operation during route discovery would not attempt to disrupt the actual data transmission at a later time.

SRDP [5] allows the source to securely discover an authenticated route to the destination using either aggregated message authentication codes (MACs) or multi-signatures. Aggregation is essential as it allows to compress authentication tags thus saving bandwidth and reduces verification costs. It uses forward and backward authentication to authenticate the route. In this protocol source node has to verify all MACs attached with a route reply (RREP) message, produced by the intermediate nodes. Hence, the verification cost at the source node increase with the route length.

Key Management (KM) and Secure Routing (SR) are two most important issues for MANETs. Secure routing ensures successful routing among authentic nodes with adversary nodes existing around or inside the networks. Key management provides key generation and distribution methods and ideally key protection and revocation. KM-SR [6] uses identity based cryptography (IBC) and provides security features such as confidentiality, integrity, authentication, freshness and non-repudiation. It is secure because uses 1-to-m broadcast key instead of only one group broadcast key and has less keys to store per node due to using asymmetric keys instead of pairwise symmetric keys. Compared to PKI

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

solutions the storage and communication requirements are lower due to IBC properties. Compared to previous IBC solutions it has no KM-SR interdependency cycle problem and is immune to inside attacks and mobile attacks and many routing attacks. It uses computationally expensive digital signatures to authenticate the routing messages so it is not suitable for resource constraint MANETs.

The HEAP [7] and SEAODV [8] protocols use symmetric key cryptography for authenticating routing control packets. In the HEAP protocol [7] by using public key certificates, a node exchanges keys with its new neighbors. Excessive usage of public key certificates for key management is a drawback of the protocol. In the SEAODV protocol [8], the key distribution mechanism is highly bandwidth consuming as each node distributes a group transient key (GTK) encrypted with the pairwise transient keys (PTKs) of its neighbors.

In an Efficient Authentication and Signing of Multicast Streams over Lossy Channels [9], two efficient schemes TESLA short for Timed Efficient Stream Loss-tolerant Authentication and EMSS short for Efficient Multi-Chained Stream Signature are proposed. TESLA offers sender authentication, strong loss robustness, high scalability and minimal overhead at the cost of loose initial time synchronization and slightly delayed authentication. EMSS provides non-repudiation of origin, high loss resistance and low overhead at the cost of slightly delayed verification.

The IDS protocols are designed to detect the inside attackers. IDS protocols are classified into three categories, those are, behavior based IDS, signature or pattern based IDS and specification based IDS.

Marti et al. [10] have proposed a behavior based watchdog mechanism where each network node overhears the transmissions of all its neighbors to detect their routing misbehaviors. But the drawback of watchdog mechanism is that it only works with Dynamic Source Routing (DSR) , watching the forward node on the path from source to destination. In On Intrusion Detection and Response for Mobile Ad Hoc Networks [11] they presented network intrusion detection (ID) mechanism that rely upon packet snooping to detect aberrant behavior in in mobile ad hoc networks. They presented two response mechanisms which are passive and active. In passive response if a node finds any intrusive node then it raises an alarm and removes that intrusive node from its neighbor table and will no longer participate in route discoveries, Hello Messages or collaborative routing with the intrusive node. When a node raises an alarm in active response then the node forwards that alarm to all of its cluster heads. Then the cluster head initiates the voting scheme and active responses to intrusions. But the voting scheme can fail if most of the cluster heads are in fact malicious nodes. In this Intrusion Detection mechanism a mis-route cannot be determined but any modification to the packet or dropping of the packet can easily be recognized and logged.

III. CONCLUSION

A mobile ad hoc network consists of several mobile nodes with computing and communication capabilities where each node works as a sender as well as a receiver and meanwhile as a router as well. Different routing algorithms have been designed for secure communication. As this is a very vast area we have only surveyed and summarized different authentication based secure routing protocol and intrusion detection secure routing protocol. Each of these secure routing protocols have their own advantages and pitfalls. Further research can be done to find the best possible optimal routing approach which will be promising in terms of energy efficiency as well as concerned with optimizing and healing paths to reduce the number of hops while providing the security.

IV. ACKNOWLEDGEMENTS

Sincere thank to the reviewers for reviewing this manuscript and providing inputs for greatly improving the quality of this paper.

REFERENCES

1. Shrikant H Talawar, Soumyadev Maity and R. C. Hansdah , " Secure Routing with an integrated localized key management protocol, in MANETs", International Conference on Advanced Information Networking and Applications, pp. 605-612, 2014.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

2. L. Chen, J. Leneutre, and J. J. Puig, "A secure and efficient link state routing protocol for ad hoc networks", In Proc. of the International Conference on Wireless and Mobile Communications (ICWMC), pp. 36-36, 2006.
3. K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "Authenticated routing for ad hoc networks", IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 598- 610, 2005.
4. 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 Simulation Conference (CNDS), pp. 193–204, 2002.
5. J. Kim and G. Tsudik, "Srdp: Secure route discovery for dynamic source routing in MANETs", In Proc. Of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, vol. 7, no. 6, pp. 1097 – 1109, 2009.
6. S. Zhao, R. Kent, and A. Aggarwal, "A key management and secure routing integrated framework for mobile ad-hoc networks", Tenth Annual International Conference on Privacy, Security and Trust, vol. 11, no. 3, pp. 1046–1061, 2013.
7. R. Akbani, T. Korkmaz, and G. Raju, "Heap: A packet authentication scheme for mobile ad hoc networks", Conference on Ad Hoc Networks, vol. 6, no. 7, pp. 1134 – 1150, 2008.
8. C. Li, Z. Wang, and C. Yang, "Secure routing for wireless mesh networks", International Journal of Network Security, vol. 13, no. 2, pp. 109–120, 2011.
9. Perrig, R. Canetti, D. Song, and J. Tygar, "Efficient and secure source authentication for multicast", In Proc. of the Network and Distributed System Security Symposium (NDSS), vol. 1, pp. 35–46, 2001.
10. S. Marti, T. J. Giuli, K. Lai, M. Baker et al., "Mitigating routing misbehavior in mobile ad hoc networks", In Proc. of the International Conference on Mobile Computing and Networking, vol. 6, no. 11,, pp. 255–265, 2000.
11. J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks", In Proc. Of the IEEE International Conference on Performance, Computing, and Communications, pp. 747–752, 2004.

BIOGRAPHY

Komal Madhukar Khedkar is a M.E. student in the Computer Engineering Department, Dhole Patil College of Engineering, Pune University. She received Bachelor degree in Computer Science and Engineering stream (B.E.-C.S.E.) in 2012 from BAMU, Aurangabad, Maharashtra, India. Her research interests are Mobile Ad Hoc Networks, Algorithms etc.