International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.2, No.3, March 2013 DOI:10.15693/ijaist/2013.v2i3.29-33

Secured Position Based Routing Protocols for Mobile Ad Hoc Networks: A Survey

B.Rammyaa[1], Dr.Sumathi Poobal[2]
Assistant Professor[1], Professor[2]
Department of ECE,
Kcg College of Technology, Chennai.

Abstract – Mobile Ad hoc Networks are particularly used in critical applications that lack fixed Network infrastructure. The geographical information used by routing protocols makes forwarding decision for reduced routing. But the topology based MANET protocols are vulnerable to number of attacks. As position based routing protocols concentrate on improving the performance, they fail in the security issues. Current position based routing allows anyone within the range to receive the position information and cannot be designed for use in high risk environment. If lots of authentication techniques are implemented, the battery power of the nodes gets exhausted. The objective of the paper is to compare different secured position based routing protocols to find solution for secured routing.

Keywords – **MANET, routing protocols.**

I. INTRODUCTION

A mobile Ad hoc network (MANET) is a collection of wireless mobile nodes self- configured to form an infra-structure less network. It is important that the routing protocol should be able to find routes that have a high degree of mobility. The challenges to the routing protocol design are the lack of dedicated routing infrastructure. Routing is the process of finding a path from a source to some arbitrary destination on the network. Existing routing protocols can be classified either as proactive or reactive. Routing in MANET is an important issue as it involves sending messages to a destination node in a network. As each node move arbitrarily in MANET, it causes the network topology unpredictable as it change frequently. These characteristics make the designing of routing protocol more complicated for MANET. MANETs can quickly set up as needed and they need secure routing than any other network due to lack of infrastructure and broadcast nature of the network. Position based routing protocols can offer significant location information for making forwarding decision. Lack of privacy in position based routing algorithm is due to exposure of position information. In this paper various routing protocols based on their position and security issues are discussed.

In Section II we discuss related secure and position based routing protocols. Section III, Overview the details of comparison and discussion of different protocols and Conclusion in Sections IV.

II. REVIEW OF SECURE POSITION BASED ROUTING PROTOCOLS

Position changes which occur because of nodes mobility in MANET cause changes in routing tables of nodes. Localization is realized by GPS that is used to determine geographical positions of nodes. The GPSs, which are embedded in nodes, are used to update information in tables in position-based algorithms. That makes position-based algorithms different from the table driven and on demand algorithms. Routing protocols uses geographical information to make forwarding decisions, resulting in reduced routing.

One of the primary applications of MANETs is in military use. In high risk environment position information broadcasted allows anyone including enemy within the range to receive the information. So the position used in MANET routing protocols are to be protected. Secure routing protocols protects routing messages against malicious nodes.

A. Secure Routing Protocol (SRP)

In [9], Papadimitratos and Haas propose the Secure Routing Protocol (SRP) as a solution for securing MANET. SRP requires a security association between the source and destination nodes and asserts that SRP guarantees the node initiating a route discovery will be able to identify and discard replies providing false topological information, or, avoid receiving them. Any two nodes that wish to communicate securely can establish a shared secret by using routing protocol modules. to a base reactive protocol, such as AODV.

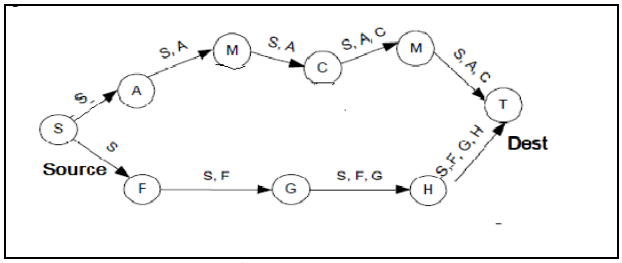

Fig 1. Example for SRP routing.

Data and trusted values are routed only through trusted node. The true shortest path requires 4 hops in the above figure 1 example. The source node will not choose the shortest path because it believes in the false path of 3 hops. If this false path is choosen, the malicious nodes negatively impact the network performance by delaying or dropping packets. The protocol violates security requirements. Hence poor performance may continue since it appears to be shortest path.

B. Security Aware Ad Hoc Routing (SAR)

The SAR protocol is an extension of existing on-demand ad-hoc routing protocols. This protocol [6] uses different approach. The nodes are assigned trusted values and the data are routed only through trusted nodes. The source sends a RREQ with embedded certain security attributes and trust levels defined by the user. Only those nodes that satisfy the required level of security can participate in the routing protocol. Nodes that do not meet the requested security requirements must drop the RREQ. If a route satisfying the requested security attributes does not exist, the protocol initiator can choose to send another RREQ with modified security attributes to find a route with different security.SAR is flexible in that it may be used in many different ad hoc environments. This approach is resource demanding but it is a useful mechanism for prevention of attacks.

C. Secure Position Aided Ad Hoc Routing (SPAAR)

SPAAR was designed for use in a specific environment. In [2], the ad hoc networks are classified into three environments: open, managed-open, and managed-hostile. Each environment differs in its security needs and opportunity for pre-deployment coordination. SPAAR targets an environment similar to *managed-hostile* environment. The *managed-hostile* environment is described as a MANET formed by military nodes in a battle environment or, similarly, an emergency response crews in a disaster area. Nodes are generally deployed from a common source and the opportunity for the pre-deployed security parameter exchange often exists.

Sensitive information is passed between nodes, and malicious nodes are a constant threat. It is important to distinguish malicious nodes from compromised nodes. A malicious node to be an unauthorized node disrupts the network. SPAAR uses encryption to prevent attacks, though at the expense of performance and resource consumption.

A compromised node to be an authorized node deployed by a known source. A compromised node may or may not engage in malicious activity or misbehave. As a result, detection of compromised nodes can be very difficult. In many cases it is difficult to distinguish malicious activity by a compromised node from legitimate node activity. SPAAR protects a MANET from attacks by malicious nodes, while attempting to minimize the potential for damage by attacks originating from compromised nodes. While SPAAR does not defend against all malicious activity from compromised nodes, ad hoc intrusion detection systems, such as [9], can help to identify compromised nodes.

SPAAR provides the necessary elements to secure routing in a high-risk environment: authentication, non-repudiation, confidentiality, and integrity. The protocol protects position information via cryptographic techniques. The protected position information is used to reduce routing overhead and increase the security of routing.

D. Security Grid Location Service Forwarding (SGLSF)

The SGLSF [16] mechanism combines Secure Geographic Forwarding (SGF) [17] and Grid Location Service (GLS) [8]. The SGF mechanism uses the shared key and the Timed Efficient Stream Loss-tolerant Authentication (TIK) [18] protocol to provide source authentication, neighbor authentication, and message integrity by incorporating hashed message authentication code (MAC1). By combining these SGF and GLS, SGLSF, enhances the security to the original protocol to ensure that any receiver can authenticate the accuracy of location messages. SGLS has the ability to message tampering, dropping, falsified injection, and replay attacks.The Local Reputation System (LRS) find compromised and selfish users and isolate messages by dropping attackers from the network. Both mechanisms combined; continue to maintain a larger message delivery ratio at the expense of a slightly higher average end-to-end delay and routing overhead compared to when they are not combined. SGLS can operate efficiently by using effective cryptographic mechanisms.

E. Secure Ad hoc Routing Protocol

Most of the attacks on routing protocol are due to absence of Encryption. Unauthorized modification of such fields could cause serious security threats. DES for encryption mechanism is used. Each node in the network maintains a public/private key pair; the certificate is to be valid for certain time period. Each node has T's public key, so it can decrypt certificates of other nodes. The protocol overcomes all known vulnerabilities of the existing prot ocols. It uses DES encryption mechanism to secure the fields in routing packets. The most severe attacks on MANETs is warm hole attack. This can be overcome applying efficient secure neighbor detection mechanism. To enhance the security level of discovered path, route selection is done based on trust level of nodes along the path. In order to secure position coordinates of each node Position verification system is employed.

Based on the basic operation of AODV as in figure 2, the protocol follows different routing mechanism based on the security level required by application. In mode 1, the packets are routed along the trusted path based on the trust

factor of the nodes. In mode2, the packets are routed along the shortest path based on hop count. The protocol uses a mechanism to detect and overcome the effect of falsified position information in geographic routing position.

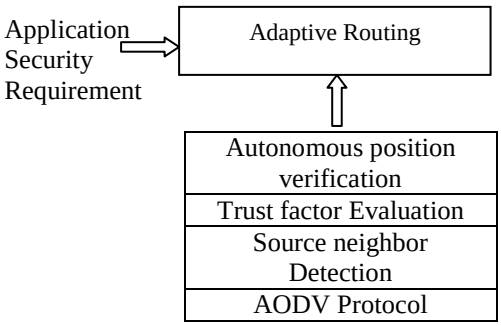

Fig 2. Conceptual Framework

The protected position information reduces the routing overhead and increase the security of routing.

F. PRISM PROTOCOL

Privacy-friendly Routing [5] in Suspicious MANETs protocol (PRISM) is an anonymous location-centric on-demand routing protocol based on three main building blocks: (1) the well-known AODV routing protocol, (2) any secure group signature scheme (or one time public key certificates), and (3) location information. PRISM is fundamentally different from all prior anonymous on-demand MANET routing protocols on two accounts: (1) PRISM uses a location-centric, instead of an identity-centric, communication paradigm. Therefore, it does not assume any knowledge of long-term node identifiers or public keys. (2) PRISM requires neither pre-distributed pair wise shared secrets nor on-line servers of any kind. PRISM reveals less of the topology and is thus more privacy-friendly.

G. SECURITY ARCHITECTURE FOR MANETS

Security issues in mobile ad hoc networks. The designing of security architecture[6] for tackling security challenges mobile ad hoc networks are facing is discussed. The security architecture in a layered view is analyzed for such applying the security architecture in military scenarios. It can be used as a framework when designing system security for ad hoc networks. An efficient secure routing protocol for mobile ad hoc networks guarantees the discovery of correct connectivity information over an unknown network, in the presence of malicious nodes in term of anonymous location-based routing in certain types of suspicious MANETS. It relies on group signatures to construct one-time pseudonyms used to identify nodes at certain locations.

The framework works with any group signature scheme and any location-based forwarding protocol can be used to route data between nodes. Also in Alternate routes are utilized only when data packets cannot be delivered through the primary route. As a case study, this algorithm is applied to AODV for performance improvements.

III. COMPARISION OF THE PROTOCOLS

Secure communication is a major concern in wireless ad hoc networks due to the broadcast nature of the of network, the existence of a wireless medium, and the lack of any Centralized infrastructure. Multicast routing protocols should take this into account, especially because some of these protocols are applied in areas such as military (battlefield) operations, national crises, and emergency operations. The unique characteristics of MANETs, combined with security threats, demand solutions for securing ad hoc networks prior to their use in commercial and military applications. Some of the unique characteristics of MANETs that pose a strong challenge to the design of the secure multicast routing protocols include: open peer-to-peer network architecture, shared wireless medium, demanding resource constraints, and dynamic network topology.

Routing is a challenging aspect of moving packets around in a network. It is a significant problem because any node can perform the role of the router in MANET and security concepts were not included into the routing protocols when they were designed. It is important because the routing table forms the basis of the network operations . The comparison of various algorithms based their routing protocols, mechanism and optimization of the result is done in Table 1. Each algorithm has its own pros and cons. Among several security protocols, no approach fit for all networks, because the nodes can vary between any devices.

MANETs lack fixed infrastructure and nodes are powered by batteries with a limited energy supply. Nodes stops functioning when the battery drain It is a difficult challenge to provide energy efficiency as it is impossible to recharge or replace a mobile node, powered by battery during mission. Hence energy efficiency is an important consideration. Traffic should be routed in the way energy consumption is minimized. Energy saving techniques aims at minimizing total power consumption. this can be done by minimizing the control overhead, maximizing the lifespan.

.

Table1: Comparision of Protocols

Name of the Approach	*Protocol*	*Assumption*	*Result Optimisation*	*Technique Used*
Secure position based routing protocol (Hybrid)	SGF (Secure Geographic forwarding) mechanism and	Effective cryptographic mechanism	Souce authentication, Neighbor authentication and message integrity	Ns-2 simulator
Secured Position Aided Ad hoc Routing	SPAAR (Secure Position Aided Ad hoc Routing)	Cryptographic techniques	Authentication, privacy , overall routing overhead reduction and integrity.	Asymmetric Cryptography
Five Layer Security Architecture	PseudoAODV protocol	Security architecture for MANETs	Designing security architecture, tackling security challenges	Case study of five layered architecture
Privacy-Preserving Location-Based On-Demand Routing	PRISM (Privacy friendly Routing in suspicious MANETs protocol)	Location centric Communication	Privacy, security, efficiency and Authenticate node	Network simulator
Secure Routing Protocol for securing MANETs	SRP(Secure Routing Protocol)	Data and trusted values routed through trusted routes	Discards false topological information	Secure Routing in RREQ
Security aware Ad hoc routing for Wireless Network	SAR(Secure aware Ad hoc Routing)	Nodes with security level participate in routing	Flexible and Prevent Attacks	Network Simulator
Secure On-Demand Position-Based Ad Hoc Routing	AODV protocol	Adaptive Routing, Autonomous Position verification system, Trust factor evaluation ,secure neighbor detection	Enhance security level of discovered path, overcome warm hole attack	DES encryption mechanism to secure the field in routing packets

IV. CONCLUSION

An overview of existing scenario of the routing protocols for MANETs, based on their position based secured routing is presented. Each protocol has its own advantages and limitations. The problems that exist in the network and their emerging solutions are discussed. Also a comparative study of the protocols based on Secured Position Based Routing for maintaining the location privacy routing along with efficiency of the algorithm is done. It is difficult task to compare the protocols with each other directly. Since each protocol differ in their assumption and mechanism for achieving their goal. Each protocol has its own strength and drawbacks. Ad hoc networks gain many applications today; also it's a wide area of research with the problems and emerging solution.

REFERENCES

[1] Busola S. Olagbegi and Natarajan Meghanathan, "A Review Of the Energy Efficient and Secure Multicast Routing Protocols for Mobile Ad Hoc Networks" International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.2, No.2, June 2010.

[2] B. Dahill, B. Levine, E. Royer, and C. Shields, A Secure Routing Protocol for Ad Hoc Networks, University of Massachusetts Technical Report 01-37, 2001.

[3] K. El Defrawy and G. Tsudik, "Alarm: Anonymous location-aided routing in suspicious manets," IEEE ICNP 2007, pp. 304–313, Oct.2007.

[4] Joo-han-Song, Vincent.W.S.Wong, "Secure position based routing protocol for Mobile ad hoc networks position based routing protocol for Mobile ad hoc networks" Science Direct ,June 2006.

[5] Karim El Defrawy, et al, " Privacy-Preserving Location-Based On-Demand Routing in MANETs" IEEE Journal On Selected Areas In Communications, VOL. 29, NO. 10, DECEMBER 2011

[6] Komal Chandra Joshi et al, "Secured Position Aided Ad hoc Routing Security of mobile ad hoc network with five layer security architecture'' International Journal ITT, India, Dec 2010.

[7] H. Krawczyk, M. Bellare, R. Canetti, HMAC: Keyed Hashing for Message Authentication, IETF RFC 2104, February 1997.

[8] J. Li, J. Jannotti, D.S.J. De Couto, D.R. Karger, R. Morris, A Scalable Location Service for Geographic Ad hoc Routing, Proceedings of the ACM Mobile Computing and Networking Conference, August 2000.

[9] Papadimitratos and Z.J. Haas, Secure Routing for Mobile Ad hoc Networks, Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio, USA, 2002.

[10] Perking CE;Royer EM (1999). Ad-Hoc on Demand Distance Vector Routing . Proc. Of 2nd IEEE Wksp.

[11] A. Perrig, R. Canetti, D. Song, D. Tygar, B. Briscoe, TESLA: Multicast Source Authentication Transform Introduction, IETF Internet Draft of Multicast Security Working Group (work in progress), August 2004.

[12] Pushpa Lakshmi.R "Secure On-Demand Position-Based Ad Hoc Routing through Autonomous Position Verification" Mobile and Pervasive Computing (COMPC-2008).

[13] Stephen Carter and Alec Yasinsac "Secure Position Aided Ad hoc Routing", Material based upon work supported in part by the U.S. Army Research Laboratory and the U.S. Army Research Office under grant number DAAD19-02-1-0235.

[14] Watanabe M, Higaki H (2007). No-Beacon GEDIR; Location-Based Ad-Hoc ROUTING with Less Communication Overhead. International Conference on Information Technology.

[15] J.H. Song, Load-balancing and secure routing for wireless mobile ad hoc networks, Ph.D.'s thesis, Department of Electrical and Computer Engineering, The University of British Columbia, April 2005.

[16] J. Song, V. Wong, V. Leung, Secure Position Based Routing Protocols for Mobile Ad hoc Networks, vol. 5, no. 1, pp. 76-86, January 2007.

[17] H. Krawczyk, M. Bellare, R. Canetti, HMAC: keyedhashing for message authentication, IETF RFC 2104 (February) (1997).

[18] A. Perrig, R. Canetti, D. Song, D. Tygar, B. Briscoe,TESLA: multicast source authentication transform introduction, IETF Internet Draft of Multicast Security Working Group (work in progress), August 2004.

[19] Y.-C. Hu, A. Perrig, D.B. Johnson, Packet leashes: a defense against wormhole attacks in wireless network,in: Proc. IEEE Infocom, San Francisco, CA, March/April 2003.

[20]] Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad hoc Networks, Proceedings of the 6th International Conference on Mobile Computing and Networking, Boston, USA, 2000.