International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 1 No: 3 March 2016

Larp-Protocol for Secure Location Services based on Direct Anonymous Attestation (DAA) Scheme in Manet

D.Subathra[1], V.Muthupriya[2]
[1]Post Graduate student, B.S.Abdur Rahman University, Chennai
[2]Assistant Professor (S.G), B.S.Abdur Rahman University, Chennai
[1]subaskpit@gmail.com, [2]muthupriya@bsauniv.ac.in

Abstract: Secure location services are one of the most popular applications for mobile ad hoc networks (MANET) and a hot research area. The main objective of this service is to provide secure communication between the source and destination by hiding the identities of the node and preventing attacks by external observers on traffic analysis. In this paper, we propose Location Based Anonymous Routing Protocol (LARP) using the Direct Anonymous Attestation (DAA) scheme that provides security and privacy from the attack by the intruder. The proposed routing protocol uses geographical information to hide the source, destination and route between them and to improve the possibility of attacks on location disclosure. The location based anonymous routing protocols which provide the complete protection without compromising the security and privacy. We use direct mode of communication by selecting the random path to portray the zone position of mobile nodes through hiding the node identities and making it anonymous. The DAA scheme uses two protocols for getting signed and verifies the user authentication which provides secure location services to reducing the privacy threat. Results show better performance of the proposed protocol.

Keywords: LARP, DAA, Secure location Services, Anonymity

1. INTRODUCTION

An ad hoc mobile network (MANET) is less infrastructure and a wireless network. They provide access to information and are very scalable for more nodes. They actually improve the flexibility and reliability of secure data transmission. These applications are small, dynamic and less resource when compared to wired networks. The nodes are very independent to move in the network and join the network. The mobile nodes are connected in a distributed manner can work at anywhere anyplace. There is no fixed infrastructure and dynamic topologies are created with limited bandwidth. When a node tries to send the information to another node which is out of communication range, the intermediate node is used to forward the information.. The mobile nodes broadcast their request to all the nodes in the network and dynamically creating the path. It is a self configurable and improved flexibility in nature. Mobile and spontaneous behavior requiring minimal human intervention to configure the network [5]. All nodes have the same characteristics with similar responsibilities and capabilities and are therefore completely symmetrical. The absence of fixed infrastructure, operated as a standalone Network in the mobile environment. Security in MANET plays a vital role in the network. The several security issues in ad-hoc networks are Availability, confidentiality, integrity and Resilience to attacks. Availability ensures both data and services. The assets can be available and accessible to the authorized parties. Confidentiality ensures the protected information which is exchanged. The unauthorized parties can read the messages, by implementing disclosure attack like eavesdropping, location disclosure, and etc. Integrity means the information can be read only by the authorized parties. Any intruders cannot corrupt the message is being transferred. When several nodes are compromised or destroyed from the network, resilience to attacks is required to sustain their functionalities in the network. This paper focus on confidentiality, such as location disclosure attack can obtain the location information using GPS system. The concept of hiding the location elements of the node and preventing the active attackers is anonymous in order to

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 1 No: 3 March 2016

provide secure communication between the host and the receiver. Researchers must understand various types of attacks and their effects on the environment of MANETs. Timing attack, Wormhole attack, Location disclosure attack, Sybil attack, DoS attack, Resource consumption attack, intersection attack and etc can also suffer the networks. Privacy plays a major role in Ad-hoc networks. Privacy threat is a risk that the adversary can obtain the user information using unauthorized access. Location privacy attack can degrade the performance of the network. To achieve privacy, the users need to ensure the anonymity and psuedonymity. This paper proposes the privacy framework for providing the trusted location servers to attain authentication and confidentiality. In this paper, we propose a new dynamic, secure location based anonymous routing protocol for secure transmission of mobile nodes which provides complete anonymity, security and privacy. To achieve privacy enhancing the DAA scheme for preventing location disclosure attack is proposed.

1.1 Routing Protocols in MANET

The mobile ad-hoc networks are characterized as multi hop network topology that can change frequently. So the effective routing path needed to establish a communication between the host and receiver. The routing protocols are divided into location based and non location based protocols as shown in fig 1.

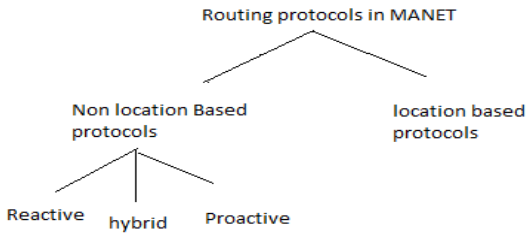

Figure 1. Routing protocols in MANET

1.2 Non Location Based Services Protocol

It is a traditional concept which maintains the table to updating the routing information. It is categorized as three groups such as proactive, reactive and hybrid. Proactive protocols (Table-driven) can update the routing information periodically in the routing table at regular interval of time [16]. Ex. Destination sequenced distance vector (DSDV). It can share the link information and maintaining the routing updates. In Reactive protocols (On -demand) can find the path dynamically such as Dynamic Source Routing (DSR) and Ad-hoc on demand Distance Vector (AODV) protocols can find out the routes instantly. If any node can fail to set the path means, it can find an alternate path for routing. In Hybrid protocol is a combination of both reactive and proactive protocols.

1.3 Location Based Services (LBS) Protocol

The location based services use the geographical information of node and broadcast their request to another node. Due to the mobility the node can move out of range, the intermediate node is used to forward the request to establish the communication. In this protocol using the random way mobility model, it assumes the node can communicate via the random path. The node tries to find another node within the transmission range to transmit the data packet to the destination. In case if any intermediate node in the transmission path fails, the protocol removes that node dynamically and set an alternate path to find the destination. Each node has a location server to maintain the position update information. Each intermediate node can acquire the position and get the location information from the location server and forward the data to the respective destination as shown in fig.2 [9].

The LBS has five components such as the service providers, the mobile agent transmit and receive device, the positioning system, the end users transmitting and receiving devices and the GPS receivers [9]. The main advantages of location based services are to establish a route randomly without storing in the routing table and thus which reduces the routing overhead in the network.

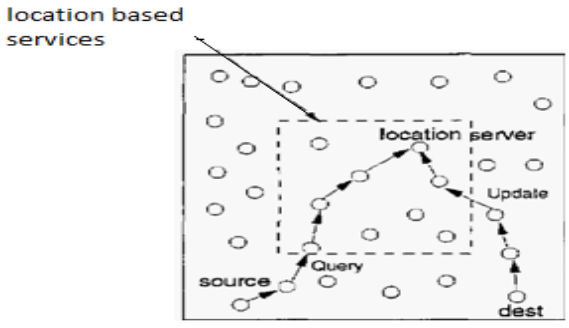

Figure 2. Location based services

1.4 Security Issues in LBS

Security plays a vital role and also challenging issues in MANET. The Ad-hoc networks are exposed to different types of attacks such as active attacks and passive attacks. The malicious observer may try to compromise the location server; it contains the public key and location of the destination. When the user report their location to update the database continues to entertain the location server. In case if the LBS then untrustworthy provides the location information to the attacker and it will pose a major privacy threat. Then the performance of the protocol is degraded.

2. LOCATION DISCLOSURE ATTACK

Greedy Perimeter Stateless Protocol (GPSR) is the geographic routing protocol, which provides the location information and also offers the route, the identity and location anonymity of source and destination [17].The location disclosure attack is possible at the network layer which gathers all the node location information using GPSR. Each node utilizes the geographic location of nodes and gains the knowledge about the location of another node. Thus, it makes the attacker node to easily know about the location of the sender and receiver. Thus can able to expose all the node locations to the intruders. In location based services assumes that each node know its own location using GPS systems by exchanging hello messages. In the end, the attacker knows which nodes are situated on the route to the target node. If the location of some intermediate node is known, one can gain the information about the location of destination as well. This attack can degrade the performance of the proposed system.

3. RELATED WORK

The Anonymous Routing protocols are as follows, L.Y. Zhao et al. [1] The proposed Anonymous Location-Based Efficient Routing Protocol (ALERT) uses unidentified routing protocols that hide node identities and routes from external observers to protect anonymity. However, existing anonymous routing protocols, which rely on either hop - by - hop encryption or redundant congestion, are either costly or can not provide full anonymity for data sources, destinations and routes. The protocol is not a complete bulletproof to all attacks. A. Inomata et al. [2] Proposed a protocol An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks that provides traffic analysis, which an attacker determines a target node and conducts an intensive attack against it, called target-oriented attack. The traffic inquiry and the target-oriented attacks are known as quite severe problems in MANETs, including position-based routing protocols, with admiration to the degradation of both throughput and security of the routing. Also position information of routing nodes is very sensitive data in MANETs. K.E. Defray et al. [3] Proposed a protocol Anonymous Location-Aided Routing in Suspicious MANETs; where nodes establish communication based on long-lasting public identities. ALARM uses nodes' current areas to securely disseminate and construct topology snapshots and forward data. With the aid of advanced cryptographic technologies (e.g., group signatures), ALARM provides both security and privacy features, including node verification, data integrity, mystery, and intractability (tracking-resistance). G. Tsudik et al. [4] Proposed protocol called PRISM: Privacy - friendly routing in suspicious MANETs focuses on mobility's privacy aspects. In contrast to most networks, where communication is based on long - term identities (addresses), the location is centric. These protocols can only focus on anonymity and the next section will focus on the secure location services is proposed.

4. PROPOSED SYSTEM

To overcome the existing problem of location disclosure attack and the privacy threat, The Location based Anonymous Routing Protocol (LARP) is proposed which provides secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. It incorporates the major consequences of ALERT protocol, but certain functionality will be differ [1]. The LARP can dynamically partition the network fields into zones and randomly selects the path, which form a non traceable anonymous route is shown in fig.3. Each node uses a dynamic pseudonym as its node identifier rather than using its real MAC address, which can be used to trace the node's existence in the network. Each node has a separate location server. Each position update is maintained at the location servers. To provide the secure location services using DAA scheme and preventing location disclosure attack is the main functionality of LARP. It can achieve better efficiency when compared to GPSR protocol. In this paper, we presented the secure location services using a

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 1 No: 3 March 2016

Direct Anonymous Attestation Scheme, which provides the complete anonymity protection with privacy enhancement. The attestation scheme should be verified and protect the information and it's anonymous. It cannot bulletproof to all the attacks. Furthermore, we can control the location disclosure attack using the secure location based services. The effective performance of LARP can be compared with ALERT

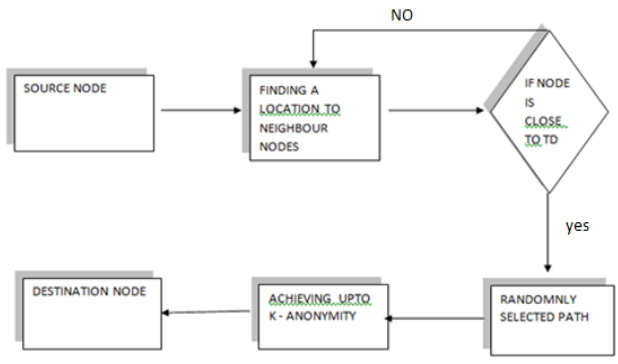

Figure 3. Flow graph of LARP

Impact of Location Disclosure Attack in LARP

When the source node uses the LARP protocol for data transmission at random paths is formed in the network. Once the attacker can select the intermediate node to target the destination to obtain the location information using location servers. The untrustworthy location servers can give the location details to the attacker. The location server contains the public key and destination zone position. When the attacker can gain all the information about the location of destination issues the major privacy threat. The privacy threat in three groups such as targets the private information, obtaining the message exchanged by service provisioning, the nature and inference knowledge to attackers. Due to this attack, the nature of LARP protocol is ruined. The next section deals with the prevention of location disclosure attack.

5. PREVENTION SCHEME

The location disclosure attack can be prevented by providing the secure location service using the Direct Anonymous Attestation scheme [9]. In this scheme provides confidentiality and privacy of mobile users. This framework can provide privacy in location based services and also this method is used in Privacy Enhancement in Location Based Services (PE-LBS) framework. The secure location server is needed to attest all the nodes to achieve confidentiality. The scheme gives to prevent from the disclosure attack, the scheme uses two protocols for the sign and the verify the intruders. The attestation is very important concepts to aware of neighboring node are identified and got signed from the trusted nodes and making as anonymous. The DAA method can able to distinguish between the valid and fake messages. The DAA allows the anonymous communication between the issuer and the verifier to obtain the secret credential value of the authentication. This scheme uses two protocols such as join protocol and sign protocol.

Join protocol: This protocol can communicate between the sender and the issuer to build an anonymous credential value.

Sign protocol: This protocol can communicate between the sender and the verifier to build an attestation certificate. The DAA scheme verifies several zero knowledge proofs to guarantee the privacy is shown in fig.4.

Attestation is the ability of showing whether the node configuration is authenticated or not It maintains the location service must be secure. Then the attestation to prevent the node identities from the active attackers.

The DAA framework provides the attestation scheme which measures the trust ability, anonymity and privacy. This can be done by verifying the intermediate nodes while running the location based services.

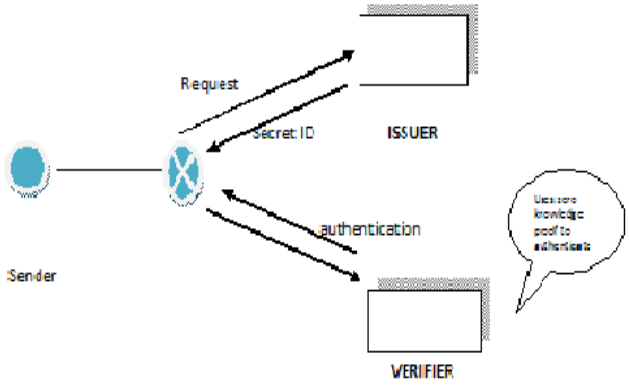

Figure 4. Architecture of DAA

Algorithm for the prevention scheme:

Step.1: The source broadcasting the request to its neighboring nodes in the zone.

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 1 No: 3 March 2016

Step.2: The source checks the neighbor node using DAA scheme to verify their proof.
Step.3: The intermediate node can obtain one secret Id to authenticate as a trusted node for data transmission.
Step.4: After verification the data can be forward to temporary destination.
Step.5: if it not authenticated, discard the node and forward the packet to another node in the network for creating a random path to deliver the packet to original destination.

6. RESULTS AND ANALYSIS

The analysis and implementation of Location based Anonymous Routing Protocol (LARP) is carried out using network simulator NS2.In this simulation, the experimental model is built on 100 nodes and the mobile nodes follow the random way point mobility model. The channel capacity is 2 Mb/s and the maximum communication range is 250 m. Other simulation parameters included in the simulation is summarized in the Table 1 below.

Table 1. Simulation Parameters

Parameter	Value
Simulator	NS2
Number of nodes	100
Traffic type	CBR
Channel type	Channel/Wireless Channel
Network interface type	Phy/WirelessPhy
MAC type	MAC/802_11
Interface queue type	Queue/Drop Tail/PriQueue
Antenna model	Antenna/Omni Antenna
Routing Protocol	LARP

6.1 Performance Evaluation

Here in this project performance comparison is done between LARP and ALERT in order to test the efficiency between them. This performance comparison is done by taking into account the performance metrics like PDR, TR, and Jitter. While making comparison LARP is proven to be highly secure and efficient one than ALERT.

Table-2 performance metrics

# t	S	R	RTR	PDR	Through put	Jit
10	51	50	150	98.039216	0.980392	4.000000
20	151	149	452	98.675497	0.986755	4.033557
30	251	249	752	99.203187	0.992032	4.020080
40	351	349	1054	99.430199	0.994302	4.020057
50	451	449	1354	99.556541	0.995565	4.015590
60	551	549	1654	99.637024	0.996370	4.012750
70	651	649	2035	99.692780	0.996928	4.135593
80	751	749	2354	99.733688	0.997337	4.142857
90	851	849	2654	99.764982	0.997650	4.126031
100	951	949	2954	99.789695	0.997897	4.112750
110	1051	1049	3254	99.809705	0.998097	4.102002
120	1151	1149	3555	99.826238	0.998262	4.093995
130	1251	1249	3855	99.840128	0.998401	4.086469
140	1351	1349	4155	99.851962	0.998520	4.080059
150	1451	1449	4455	99.862164	0.998622	4.074534
160	1551	1549	4755	99.871051	0.998711	4.069722
170	1651	1649	5055	99.878861	0.998789	4.065494

6.2 Performance comparison between LARP and ALERT

In this section, we evaluate the LARP efficiency compared between the ALERT, GPSR and some anonymous routing protocols with 100 and 200 nodes respectively. In this fig 5 as taken from [1] is compared with LARP. We use the following metrics to assess anonymity and privacy performance.
a) Ratio of packet delivery: The ratio of the number of packets delivered to the destination is defined. The LARP has considerably high packet delivery ratio i.e. 92% than ALERT.
b) Throughput: It is defined as the successful rate of packet delivery to the respective destination. It basically calculates the time slot as shown in table 2. The time taken to complete the packet delivery ration is also considered. The LARP gives the high successful rate than GPSR.
c) Jitter: The deviation of node in some aspects of high frequency. The jitter can consider the amplitude, time phasing and weak signal.
d) Number of Node Participation: The number of node can participate in the communication channel is also considered. The Random forwarders and more than 200 nodes can participate in the network zones. In fig.5a. represents the actual participation of nodes with transmitted packets respectively. It can compared with several anonymous routing protocols such as ALARM, GPSR and ALERT etc. as shown in fig.5.b

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 1 No: 3 March 2016

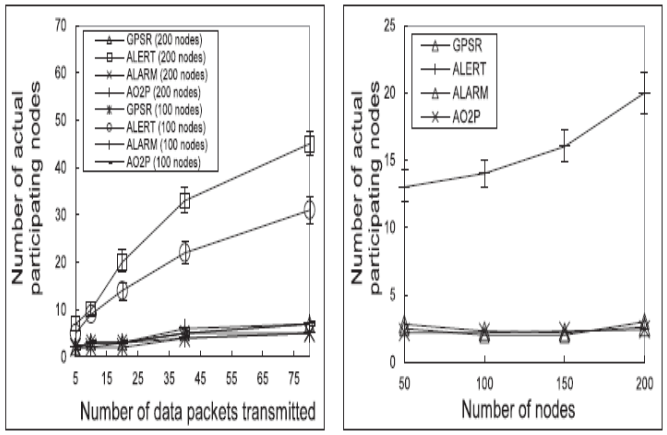

Figure 5. a) Data transmission 5.b) participation of nodes

6.3 Effect of Mobility

In this section, we observe that the simulation to obtain the major difference in LARP Performance such as Packet Delivery Ratio (PDR), throughput and jitter. In this fig.6 shows that the increasing number of throughput for delivering the successful messages in a communication channel.

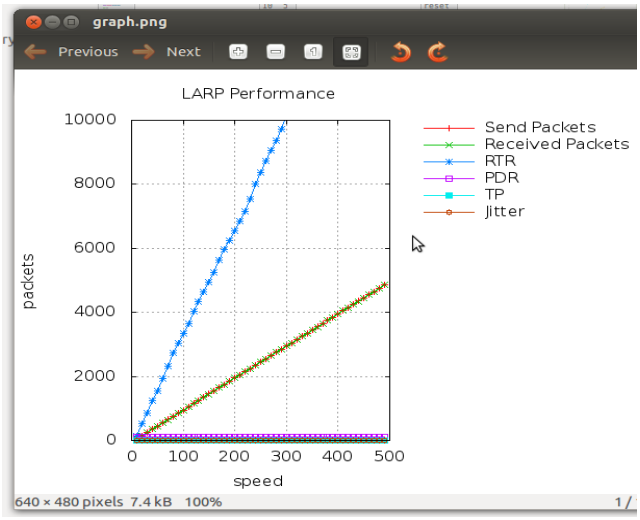

Figure 6. LARP Performance graph

The graph shows the effectiveness of LARP protocol can be taken as more than 100 nodes are participated in the network. The transmission range between one to another node is 250m.

VII. CONCLUSION

To determine the location disclosure attack in the network is formed is very critical part in MANET, because there is no infrastructure and vast openness in the system. The LARP protocol cannot bulletproof to all the attacks. This DAA scheme prevents the location based services must be secure. When the attacker can gain the knowledge about the location of node is identified and monitoring by the proposed scheme. The LARP protocol provides the secure communication to hiding node elements and authenticate by the attestation protocol. To achieve privacy for avoiding the untrusted location based services. Finally experimental work shows that the effectiveness of the proposed scheme and the complete anonymity protection .This type of attack can be prevented by this DAA scheme. The future work relies on enforcing the high reliability and confidentiality on multiple paths.

REFERENCES

[1] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", Proc. Int'l Conf. Parallel Processing (ICPP), 2011

[2] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks", Proc. Int'l Symp. Applications on Internet (SAINT), 2006.

[3] K.E. Defrawy and G. Tsudik, ALARM: Anonymous Location- Aided Routing in Suspicious MANETs, Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007.

[4] K.E. Defrawy and G. Tsudik, PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs), Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008.

[5] J. Broch, D.A. Maltz, D.B. Johnson, Y.C. Hu, J. Jetcheva, A Performance comparison of multi-hop wireless ad hoc network Routing protocols, in: Proceedings of the 4th ACM Mobile Computing and Networking Conference, October 1998, pp. 97.

[6] L. Sweeney, "k-Anonymity: A Model for Protecting Privacy,"Int'l J. Uncertainty Fuzziness Knowledge-Based Systems, vol. 10, no. 5, pp. 557-570, 2002

[7] X. Wu, "DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks: Research Articles,"

Wireless Comm. and Mobile Computing, vol. 6, pp. 357-373, 2006.

[8] A.R. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-Aware Services," Proc. IEEE Second Ann. Conf.Pervasive Computing and Comm. Workshops (PERCOMW), 2004.

[9] C. Y. Chow, "Privacy-Preserving Location-based Services" A dissertation submitted to the faculty of the graduate school of The university of Minnesota in partial fulfillment of the Requirements for the degree of doctor of philosophy may, 2010

[10] J. C. Ernie Brickell, Liqun Chen, "Direct Anonymous Attestation, "In Proceedings of 11th ACM Conference on Computer and Communications Security, ACM Press, 2004.(CCS'04), October 25-29, 2004.

