IJCSN International Journal of Computer Science and Network, Volume 5, Issue 3, June 2016
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 1.02

Hybrid Approach for Anonymity based Secured Routing in MANET with Effective Resource Utilization

[1] Charulata Ahir, [2] Dr. Hemant Deshmukh

[1] I/C Head IT dept. Govt. Polytechnic, Murtizapur.

[2] Head Computer Science and Engg. IBSS college of Engg., Amravati, Maharashtra , India.

Abstract - In current scenario MANET are the upcoming solution for communication in various fields, but the problem of security lays a prime issue. Due to the infrastructure less mode of communication such networks have good utilization in future, but due to resource constraint these network find limitation in utilization. Due to dynamic nature of nodes and variant routing property, any fixed approach for anonymity based security or resource utilization is not applicable. Hence to optimize the utilization of MANET for real time a hybrid approach is to be developed. In this paper anonymous location based routing protocol 'ALERT' and a spectrum sensing based coding in cognitive radio network called 'LAUNCH' protocol are studied and compared so as to propose a hybrid approach of providing anonymity based security with optimal resource allocation using cognitive radio network approach.

Keywords – *MANET (Mobile Adhoc Network), Anonymity, ALERT(Anonymity Location Based Efficient Routing Protocol), LAUNCH(A Location-Aided Routing Protocol for Cognitive Radio Networks).*

1. Introduction

As an evolving mode of communication for long range communication, MANET has come out as a very effective mode of communication. Due to non dependency on infrastructures, such networks are very rapidly emerging. While MANET has high portability in communication due to its self generating properties, such networks are limited with the selection of routes and their offering properties. However, various researches were made to outline an efficient routing protocol for progressive data transfer in Mobile Adhoc- network. In various approaches of route discovery in Adhoc- network, routing with security concern is upcoming. In such a network where each node is an active participant with the possibility of entering and leaving the network at any instance, reliability over the node for communication plays an important role. In various securities based routing approaches [1],[2],[3],[4],[5],[6],[7],[8] anonymity is provided to offer security at each node level. Anonymous routing provides security in MANET by hiding node identities preventing traffic attacks [9] from external nodes. Anonymity is provided to the source identity, destination identity and forwarding route.

Various anonymity routing schemes were developed in past such as ALARM[1] , SDDR, ZAP, GPSR ,[2],[3],[4],[5],[6],[7],[8][9] etc to provide secure routing. These approaches are either node to node encryption based or a redundant routing based. These approaches are however not totally robust and are limited to provide anonymity either on source, destination or route independently. In order to provide anonymity for source, destination and route simultaneously recently a location based routing protocol called 'ALERT'[11] was proposed This approach though provides an effective means for providing security in multiple levels simultaneously, the resource constraint in MANETs and it's utilization is yet to be developed.

To optimize the resource utilization in MANETs a spectrum sensing based coding in cognitive radio network called 'LAUNCH' [19] is proposed. To optimize the resource utilization the existing adhoc network is to be remodeled in a Cognitive network model with the consideration of spectrum sensing approach for remodeling the active route selection process.

2. ALERT

2.1 Assumption in ALERT

In ALERT, the attackers can be battery powered nodes that passively receive network packets and detect activities in the neighborhood. They can also be powerful nodes that pretend to be legitimate nodes and inject packets to the network according to the analytical results from their eavesdropped packets[10].

The assumptions below apply to both inside and outside attackers.

1. Capabilities: By eavesdropping, the adversary nodes can analyze any routing protocol and obtain information about the communication packets in the neighborhood and positions of other nodes in the network. They can also monitor data transmission on the fly when a node is communicating with other nodes and record the historical communication of nodes. They can intrude on some specific unguarded nodes to control their behavior, e.g., with denial-of-service (DoS) attacks, which may cut the routing in existing anonymous geographic routing methods.

2. Incapability's: The attackers do not issue strong active attacks such as black hole. They can make entry of an external group to a proportion of all nodes. Their computing resources are not unlimited; thus, both symmetric and public/private key cannot be precisely decrypted within a reasonable time period. Therefore, encrypted data are secured to a certain degree when the key is not known to the attackers.

2.2 Dynamic Pseudonym and Location Service

In ALERT, each node uses a dynamic pseudonym as its node identifier rather than using its real MAC address, which can be used to trace nodes' existence in the network. To avoid pseudonym collision, ALERT use a collision resistant hash function, such as SHA-1 [12], to hash a node's MAC address and current time stamp. To prevent an attacker from re-computing the pseudonym, the timestamp should be precise enough (e.g., nanoseconds). Considering the network delay, the attacker needs to compute, e.g., 10^5, times for one packet per node. There may also be many nodes for an attacker to listen, so the computing overhead is not acceptable, and the success rate is low. To further make it more difficult for an attacker to compute the timestamp, ALERT increases the computation complexity by using randomization for the time stamps. Specifically, the precision of timestamp is kept to a certain extent, say 1 second, and randomize the digits within $1/10^{th}$. Thus, the pseudonyms cannot be easily reproduced. A node's pseudonym expires after a specific time period in order to prevent adversaries from associating the pseudonyms with nodes.

ALERT assume that the public key and location of the destination of a data transmission can be known by others, but its real identity requires protection. ALERT utilize a secure location service to provide the information of each node's location and public key. Such a location service enables a source node, which is aware of the identity of the destination node, to securely obtain the location and public key of the destination node.

2.3 Anonymity Protection

An Anonymous Location-based and Efficient Routing protocol ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. Specifically, in each routing step, a data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. It then randomly chooses a node in the other zone as the next relay node and uses the GPSR algorithm to send the data to the relay node. In the last step, the data is broadcasted to nodes in the destination zone, providing k-anonymity to the destination.

In addition, ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source by utilizing the secure location service. It uses the "notify and go" mechanism to provide source anonymity. In this a number of nodes send information at the same time as the source sends packets. This hides the source among other nodes and provides high anonymity protection for the source. The number of nodes in the destination zone provides destination anonymity. The number of nodes in destination depends on the node density and destination zone size.

ALERT is also resilient to intersection attacks and timing attacks

2.4 Strategy to Counter Timing and Intersection Attacks

Counter timing attacks is a way to to avoid the exhibition of interaction between communication nodes. In ALERT, the "notify and go" mechanism and the broadcasting in destination zone both put the interaction between S-D into two sets of nodes to deliberately confused intruders. More importantly, the routing path between given S-D and the communication delay (i.e timestamp) changes constantly, which again keeps an intruder away from identifying the source and destination.

ALERT provides two step strategies against intersection attack the first step reaches a number of nodes in the destination zone, but the destination is reached in the second step. Because the deliveries of pkt1 and pkt2 are mixed, a attacker observes that D is not in the recipient set of pkt1 though D receives pkt1 in the delivery time of pkt2. Therefore, the attacker would think that D is not the recipient of every packet in destination zone in the transmission session, thus foiling the intersection attack.

While developing the security approach in ALERT, nodes from one cluster to next cluster is chosen in a random basis which results in resource constraint or resource wastage and hence the nodes should be selected based on selective approaches. The selection of nodes for forwarding data with security factor, resource utilization approach needs to be developed. A new approach of wireless communication system called cognitive radios is now emerging as a high rate communication device with optimal resource utilization. The approach of cognitive radio for adhoc network based on location aided coding 'LAUNCH' is proposed

3. LAUNCH

Various methods were developed in past to achieve the objective of variant resource allocation in adhoc network. Wherein these methods are basically focused on route selection approach the spectrum availability and its utilization is not observed much. The proper utilization of wireless spectrum can improvise the quality of service. Towards the allocation of spectrum in a effective manner, a new technology has emerged in recent past, called "cognitive radio network".[14],[15],[17],[18] In such a network the spectrum is allocated based on the demanded service with the categorization of primary and secondary user. Wherein CRN are coming out to be a good solution in wireless communication under resource constraint environment, the approach is now been tested on adhoc network for its feasibility. Towards the modeling of such approach in adhoc network, in recent past an approach called "location-aided routing protocol" LAUNCH"[19] is proposed. In this approach location aided information is used to guide route discovery, maintenance, and data forwarding. Packet forwarding decisions at a node are based on the geographical position of the packets destination as well as the positions of the nodes immediate neighbors. Therefore, there is no need for discovering and maintaining explicit routes, reducing communication overhead and state information at each node. Hence, location-aided routing protocols do scale well, especially when the network is highly dynamic. Moreover, many of today's wireless devices are location-enabled and this is expected to become more ubiquitous in the future. Adding to these advantages the fact that location information of CRN nodes can be obtained via FCC Geo-location[16]-Databases or estimated via measurement accurately, these features make location-aided protocols attractive for CRNs.

Although, location-aided routing has been previously investigated in the context of ad-hoc networks, applying it in the context of CRNs has its own challenges, particularly the heterogeneity of the network having two classes of nodes: i.e. Primary user (PUs) and secondary user (SUs) with preferential treatment to PUs, optimizing path selection based on the availability of multiple channels, and the tight coupling between the routing and the spectrum management functionalities at the PHY/MAC layers.

4. Summary

Table 1 shows summary of ALERT and LAUNCH protocol

Table1: Summary of ALERT and LAUNCH protocol

	ALERT	**LAUNCH**
Neighbored node selection	Random selection	Based on route stability
Resource Utilization	Not effective	Effective
Spectrum availability & utilization	Not focused	Focused
Efficiency	Effective to provide Anonymity in MANET	Effective for dynamic spectrum utilization using CRN

5. Conclusion

To optimize the utilization of MANET for real time this paper suggest a hybrid approach of providing anonymity based security with optimal resource allocation using cognitive radio network approach. The approach of security is developed by the improvement in anonymous routing protocol, where in the computational overhead during data trafficking is focused. This coding is integrated with dynamic resource allocation based on the user allocation pattern as used in CRN. In this approach the nodes are defined as primary or secondary user based on node and link weight factor. By this development adhoc network will be made more secure with higher quality of service in data communication.

References

[1] **[K. E. Defrawy et al, 2011]**"ALARM: anonymous location aided routing in suspicious MANETs," IEEE Trans. Mobile Compute., vol. 10, no. 9, pp. 1345-1358, 2011.

[2] **[Xiaoxin Wu et al,2008]** "Anonymous Geo-Forwarding in MANETs through Location Cloaking", IEEE Transactions on Parallel and Distributed Systems, Vol. 19, No. 10, October 2008.doi 1297-1309.

[3] **[Z. Zhang et al, 2006]** "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks," IEEE Trans. Wireless Communication, vol. 5, pp. 2376-2385, Sept. 2006.

[4] **[D. Sy, R. Chen et al,2006]** "ODAR: On-Demand Anonymous Routing in Ad-hoc Networks," in IEEE Conference on Mobile Adhoc and Sensor Systems., vol.4,pp. 721-730,2006,

[5] **[X. Wu et al,2005]** "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4,pp. 335-348, July/Aug. 2005.

[6] **[Cadger et al,2013]** "A survey of geographical routing in wireless ad-hoc networks." *Communications Surveys & Tutorials, IEEE* 15, no. 2 (2013): 621-653.

[7] **[Gunasekaran et al,2013]** "SPAWN: a secure privacy-preserving architecture in wireless mobile ad hoc networks."*EURASIP Journal on Wireless Communications and Networking* 2013, no. 1 (2013): 1-12

[8] **[Karim El Defrawy et al,2011]** "Privacy-Preserving Location-Based On-Demand Routing in MANETs", IEEE Journal On Selected Areas in Communications, Vol. 29, No. 10, December 2011.doi: 1926-1934.

[9] **[Muthumanickam Gunasekaran1 et al,2013]** "TEAP: trust-enhanced anonymous on-demand routing protocol for mobile ad hoc networks", IET Information Security, IET Inf. Secur., 2013, Vol. 7, Iss. 3, pp. 203–211 203 doi: 10.1049/iet-ifs.2013

[10] **[Agrawal et al,2011]** "A survey of routing attacks and security measures in mobile ad-hoc networks." Journal of computing,vol.3,issue 1,jan-2011, ISSN 2151-9617.

[11] **[Haiying Shen et al,2013]** "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", IEEE Transactions on Mobile Computing, Vol. 12, No. 6,pp.304-313, June 2013.

[12] **[M. Elena Renda et al,2012]** "Load Balancing Hashing in Geographic Hash Tables", IEEE Transactions on Parallel and Distributed Systems, Vol. 23, no. 8, August 2012. **doi** 1508-1519.

[13] **[X. Wu,2006]** "DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks: Research Articles," Wireless Comm. and Mobile Computing, vol. 6, pp. 357-373.

[14] **[Dutta et al, 2013]**"A Routing Protocol for Cognitive Networks in presence of Co-operative Primary user."*Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on*, pp. 143-148. IEEE -2013.

[15] **[Kamruzzaman et al, 2012]** "Energy-aware routing protocol for cognitive radio ad hoc networks." *IET communications* 6, no. 14 (2012): 2159-2168.

[16] **[Robert J. Hall, 2011]**, "An Improved Geocast for Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, Vol. 10, No. 2, February 2011: 254-266.

[17] **[Chowdhury et al,2009]** "Search: A routing protocol for mobile cognitive radio ad-hoc networks." *Computer Communications* 32, no. 18 (2009): 1983-1997.

[18] **[Akyildiz, Ian F et al,2009]** "CRAHNs: Cognitive radio ad hoc networks." *Ad Hoc Networks* 7, no. 5 (2009): 810-836.

[19] **[Karim Habak et al,2013]** "A Location-Aided Routing Protocol for Cognitive Radio Networks", International Conference on Computing, Networking and Communications, IEEE, pp. 729-733,Jan-2013,doi-978-1-4673-5288-8/13