Active Attack Detection and Unavailability over ALERT Protocol in MANET

Rohini Y. Sarode.
rohini.sarode7@gmail.com

Abstract— Mobile Ad-Hoc Network (MANET) is a temporary network, consists of several wireless moving nodes, has no infrastructure or centralized access point such as base station. Security is the big issue in MANET because of its nature of openness, dynamic topology, decentralized monitoring. Anonymity is to hide the subjects among another. Anonymity is one of the solutions to avoid the attacks on the network. Anonymous Location based Efficient Routing proTocol (ALERT) which provides anonymity protection for sources, destinations and routes. It also effectively counters intersection and timing attacks. ALERT is not bulletproof to all attacks like availability and active attacks and existing solutions for active attacks had not provided anonymity protection. In this paper ALERT-APD (ALERT- Assured Packet Delivery algorithm) is proposed for availability attack and ALERT-S (ALERT Security) is for active attack detection over ALERT protocol in MANET. As in this paper MANET is protected from active attack over ALERT protocol, system will give twenty five percent more effective security and anonymity protection than existing system.

Index Terms— *Anonymity, Availability, Blackhole attack, Mobile Ad-Hoc networks, Protocol, Security,Unavailability.*

*****

I. Introduction

Anonymity is the state of hiding identity of a particular subject among many subjects. Anonymity plays an important role for security in MANET. MANETs features like dynamic topology, wireless medium, very strict resource constraints and heterogeneous resources, create many challenges for security solutions. There are various types of challenges those targets the Ad-Hoc network such as security, anonymity and scalability [9].

Existing anonymous routing protocols rely on either hopby-hop encryption or redundant traffic, which either generate high cost or cannot provide full anonymity protection of data sources and destinations as well as routes. The high cost exacerbates the inherent resource constraint problem in mobile networks, especially in multimedia wireless applications. For high anonymity protection with a low cost, an Anonymous Location-based Efficient Routing protocol (ALERT) is there. ALERT dynamically partitions the network field into the zones and it randomly chooses nodes in the zones as intermediate random forwarders, which form a non traceable anonymous route. Also, it hides the data initiator and receiver among many initiators and receivers to strengthen source and destination anonymity protection. Like this ALERT offers anonymity protection to source identity, destination identity and route identity. There are some protocols which provide source anonymity, some provide route anonymity, some provide destination anonymity, but none of these are provided complete route, source and destination identity anonymity. ALERT provides these all identity and location anonymity protection for the network. ALERT doesn't check for the availability of random forwarders. However, the unavailability of Random Forwarders (RFs) may be because of either congestion or low energy, which is not enough to transfer the data. Also, it affects the packet delivery ratio of the ALERT algorithm, but it can increase the cost of latency. The proposed simple approach of ALERT-APD algorithm can provide assurance of packet delivery by waiting for the node being available on the route, and transfer the data packets. Further paper is organized as follows, section 2 gives the literature review. The architecture of the proposed system is presented in section 3 followed by the proposed algorithms and section 4 and 5 covers results and conclusion..

II. Related Work

MANET is flexible network, it doesn't require any infrastructure or central control. MANETs use anonymous routing protocols those hide node identities and/or routes from outside observers in order to provide anonymity protection. Anonymous routing protocols are crucial to provide security.

2.1 Ad-Hoc Routing Protocols

In MANET, routing protocols contribute basic task in the likely prospect of ever present devices. Existing MANET's commercial applications are basically for military or in crisis situations. It is considered that research in MANET routing protocols will place the groundwork for prospective wireless sensor type networks as well as wireless plug-and-play devices. For MANET routing protocols uniqueness and node mobility are the challenging issues to provide communication platform, i.e., solid and dynamic [5]. Security of mobile ad hoc networks with secure routing is another challenge. There are three main types of routing protocols as proactive, reactive and hybrid as shown in fig.1. Many solutions, for routing attacks such as ARAN, AODVS, SRP,Ariadne and SEAD have been proposed for protecting popular routing protocols, such as AODV, DSDV and DSR from various passive and active attacks [2]

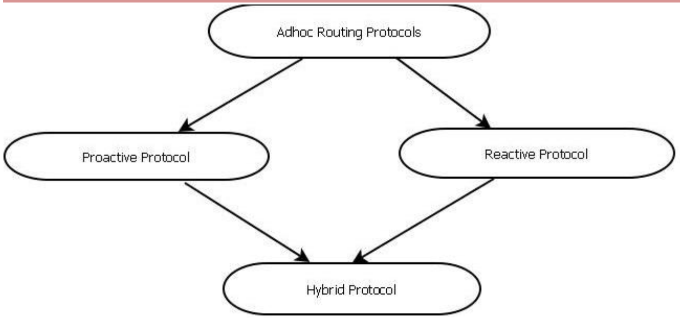


Fig. 1. Routing Protocols [8]

However, because of some inherent limitations resulting from anonymity-related requirements, those solutions cannot be employed directly in anonymous routing protocols

2.2 Anonymous Routing Protocols for Ad Hoc Networks

All Anonymous routing protocols in MANETs can be classified into following two categories: hop-by-hop encryption and redundant traffic.

Hop-by-hop Encryption:

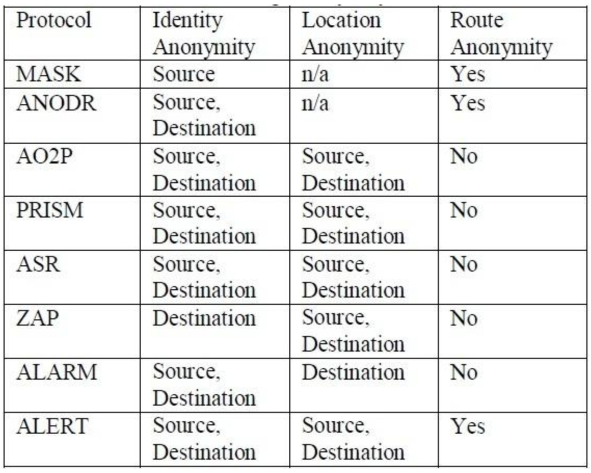
In a hop-by-hop encryption [10] a packet is encrypted during the transmission within two nodes on the way, preventing attackers from tampering or scrutinizing the contents of packet to disrupt in the communication or identify the two communicating nodes. Hop-by-hop encryption is again divided into hop-by-hop authentication and onion routing. Hop-by-hop authentication can prevent adversaries from actual participating in the routing to ensure route anonymity. In onion routing, packets encryption is done in the source node and decryption done layer by layer at each hop along the route.

Redundant Traffic:

In Redundant traffic [9], routing uses redundant traffic, such as multicasting, local broadcasting and flooding to make confusion to potential attackers. Multicast is used in the topological routing algorithm to construct a multicast tree or forest to hide the destination node in the network. MAPCP topological routing [9] uses broadcast and other geographic routing protocols also uses broadcast. Protocols like Mix Zones [4] are relying on redundant traffic.

Some anonymity protocols are forming different types of anonymity as shown in Table 1 as source or route, source and destination, destination and route but none of them are for both location and route anonymity. So ALERT is one of them, which can form location and route anonymity protection completely. ALERT [1] is distinguished because of its low cost and anonymity protection for sources, destinations and routes. Identity as well as location anonymity. This protocol uses dynamic, hierarchical partitions of zones and random relay node selection make incomprehensible to intruder, so the two end points and nodes route can't be detected. A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination.

TABLE 1
EXISTING ANONYMITY PROTOCOLS



Protocol	Identity Anonymity	Location Anonymity	Route Anonymity
MASK	Source	n/a	Yes
ANODR	Source, Destination	n/a	Yes
AO2P	Source, Destination	Source, Destination	No
PRISM	Source, Destination	Source, Destination	No
ASR	Source, Destination	Source, Destination	No
ZAP	Destination	Source, Destination	No
ALARM	Source, Destination	Destination	No
ALERT	Source, Destination	Source, Destination	Yes

ALERT-Anonymous Location Efficient Routing Protocol

The resultant different routes for transmissions make it complicated for an intruder to observe a statistical pattern of data transmission. The RF set changes due to the random selection of RFs during the transmission of each data packet. Even if an intruder detects all the nodes along a route once, adversary can't find the routes for subsequent transmissions between the same S-D pair. The anonymous path between S and D ensures that nodes on the path do not know the location of the endpoints. ALERT strengthens the privacy protection for S and D by the unlinkability of the transmission endpoints and the transmitted data. ALERT incorporates the "notify and go" mechanism to prevent an intruder from identifying which node within the source's neighborhood has initiated data packets. ALERT also uses k-anonymity to destinations by hiding D among k nodes in destination zone. Thus, an eavesdropper can only acquire information on destination zone, rather than the destination location, from the packets and nodes on the route.

2.3 Anonymity And Security Attacks

Security attacks against anonymous and secure routing in ad hoc networks can be classified into two types:

Passive Attacks:

This attack is an unauthorized entry to the routing packets or silently refusing to execute the function requested. The former type of attacks might be an attempt to gain routing information from which the attacker could extrapolate data about the positions of each node. Such an attack is usually impractical to detect.

Active Attacks:

These attack meant to humiliate or put off message flow between the nodes. They can change or stop communications and transformations of packects between nodes. Normally, such an attack involves actions performed by adversaries, the replicated, modified, and deleted data of communicating.

Routing attacks (active attacks) include blackhole, fabrication, and modification of varied fields in routing packets (request-reply messages, and error messages). These attacks could lead to serious network failure. A malicious node will interrupt the routing mechanism using following ways:

i) It modifies the contents of as exposed route,
ii) Changes a route reply message,
iii) Causes the packet to be natural as an illogical packet,
iv) It validates the route table in additional nodes by marketing wrong paths,
v) Refuses to contribute within the route finding procedure,
vi) It changes the contents of a data packet or the route.

III. Proposed System

As ALERT provides a dynamic and random routing path, which consists of dynamically determined intermediate nodes. ALERT make zone partitions repeatedly and splits the smallest zone in an alternate horizontal and vertical manner.

This partition process called as hierarchical zone based partition. ALERT uses zone partitioning and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., random forwarder), thus randomly and dynamically generated a unpredictable routing path for a message.

The system architecture is depicted in Fig.2, gives the flow of the system. It shows the idea of communication flows to reach the objective of the proposed system.

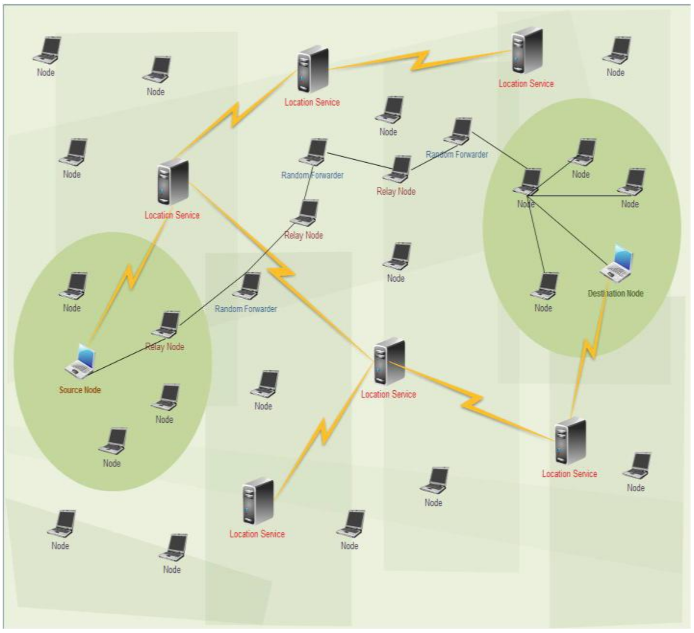


Fig 2:System architecture

3.1 Security *System Functionalities*

ALERT-APD will provide anonymity and overcome the problem of unavailability found in ALERT protocol. For the anonymity consider attacks from internal nodes (i.e. on the route) and external nodes (i.e. out of the route). It Provides identity Privacy, Location Privacy, and Route Anonymity. In the point of view of anonymity, adversaries are interested in the privacy information about the two communicating parties and exposed routes.

- *Identity Privacy:* ALERT can ensure Identity Privacy in mobile Ad-Hoc networks. In destination zone the data gets broadcasted to k different nodes, by providing k-anonymity to the destination node. In addition, ALERT has a policy to hide the data source among a number of initial nodes to increase the anonymity protection of the source.
- *Location Privacy:* The idea of recent attacks on Location Privacy is to eavesdrop the route request and route response packets and then infer the distance from the source or the destination by length checking of those packets.“Notify and go” mechanism will improve location privacy, by making uncertainty to the adversary.
- *Route Anonymity:* Current attacks on Route Anonymity are based on traffic analysis. Random selection of random forwarders with hierarchical partition route privacy is maintained.

For security over ALERT protocol, consider routing (active) attack as a blackhole attack.

- Blackhole attack is a kind of Denial Of Service (DoS) in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept.
- This attack aims at modifying the routing protocol, so that traffic flows through a malicious node controlled by the attacker. So the system’s proposed algorithm will overcome the problem of blackhole attack over ALERT protocol using proposed ALERT-S algorithm.

IV. Algorithm

The proposed ALERT-APD algorithm is as follows :

This algorithm will check unavailable nodes. If in the random route formation some unavailable nodes are finding that time it will wait for some threshold time for unavailable node to become available. Once the node becomes ready for the packet transfer it will continue path of communication.

```
1. Selection: Ns=Source Node, ND=Destination Node,
   Partition Coordinates UL={0,0}; LR={NH,NW}
2. Perform Partition Ps={H,V} (H=0, V=1)
   if(p={pt|pt=H & H E Ps})
   then UL={0,0}, LR={NH(+or-)dx, NW(+or-)dy}
    else if(p={pt|pt=V & V E Ps})
    then UL={NH(+or-)dx, NW(+or-)dy}, LR={0,0}
```

```
3. for each n E Np
        if(n.isAvailable()=true)
        then
        if(n.isDestination=false)
                n.selectedRandomForwarder=true
        go to step 2
        elseif(n.isDestination=true)
                extract packet content
        go to step 4
        else if(n.isAvailable()=false)
                then
        if(n.isDestination=false)
        then
                continue 3
        elseif(n.isDestination=true)
        while(Wait for time Twait= x seconds)
                if (Twait>x)
                then
                discard packet
        go to 4
4. Exit
```

Where,
UL= Upper Left Corner of current partitioned zone
LR= Lower Right Corner of current partitioned zone
PS= Set of partition type Boolean values
Np= Set of nodes present in current partitioned zone

ALERT-S Algorithm is as follows:

This algorithm will check the repeated entries of communications and sequence numbers generated by random forwarders. The highest sequence number of node indicates a attacking node.

```
1. Initialize,
        a. Ct = Current System Time
        b. Tt = Ct+wt
        c. HMR(snd, ni) = {}
        d. IMMN(n,i) = {}
2. while (Timer t<Tt)
        Initialize,
        a.SND= packet.destination_sequence_number
        b. NI = packet.node_ID
        Perform: HMR = HMR U (SND, NI)
3. Iterate(HMR),Initialize: i = 0
entry(isnd, ini) = =HMR(i)
if(isnd >>>> SNS)
then
        HMR = =HMR - entry(isnd, ini)
        IMMN = =IMMN U entry(isnd, ini)
4. Sort(IMMN), Criteria: SND
5. MAL_node = IMMN.max(entry)
6. EXIT.
```

V. Conclusion

Anonymity and security are the critical issues in MANET. Availability of the nodes in the network must be a big concern to be considered while anonymity and security of the Ad-Hoc network. Security can be provided in the ALERT protocol with avoiding blackhole attack. The proposed algorithm improves the packet delivery ratio, it increases the cost of latency. ALERT-S protect the network against active attack. Total twenty five percent more security protection is expanded by using the proposed system. In future, security and anonymity can be improved for prevention from active attacks.

Acknowledgment

The authors would like to thank the publishers, researchers for making their resources available and teachers for their guidance.
I also thank college authority for providing the required infrastructure and support. Finally, I would like to extend a heartfelt gratitude to friend and family members.

References

[1] Haiying Shen, Lianyu Zhao. ALERT: An Anonymous Location- Based Efficient Routing Protocol in MANETs In proccedings of IEEE transactions on mobile computing, june 2013., vol. 12, no. 6. 2013.

[2] A Zhu, Bo and Wan, Zhiguo and Kankanhalli, Mohan S and Bao, Feng and Deng, Robert H. Anonymous secure routing in mobile networks. In Local Computer Networks, 2004. 29th Annual

[3] The Kaur, Robinpreet and Rai, Mritunjay Kumar. A Novel Review on Routing Protocols in MANETs. In Undergraduate Academic Research Journal (UARJ), ISSN, pages 2278–1129.2012.

[4] Alastair R Beresford and Frank Stajano. Mix zones: User privacy in location-aware services. In Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on, pages 127–131. IEEE, 2004.

[5] Kwan-Wu Chin, John Judge, Aidan Williams, and Roger Kermode. Implementation experience with manet routing protocols. ACM SIGCOMM Computer Communication Review, 32(5):49–59, 2002.

[6] Karim El Defrawy and Gene Tsudik. Prism: Privacy-friendly routing in suspicious manets (and vanets). In Network Protocols, 2008. ICNP 2008. IEEE International Conference on, pages 258–267. IEEE, 2008.

[7] Karim El Defrawy and Gene Tsudik. Alarm: Anonymouslocation-aided routing in suspicious manets. Mobile Computing,IEEE Transactions on, 10(9):1345–1358, 2011.

[8] Mahendra Kumar, Ajay Bhushan, and Amit Kumar. A study ofwireless network attack and routing protocol attack. International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), 2(4), 2012.

[9] Xiaoxin Wu and Bharat Bhargava. Ao2p: ad hoc on-demand position based private routing protocol. Mobile Computing, IEEE Transactions on, 4(4):335–348, 2005.

[10] Lakshmi, K., et al. "Modified AODV protocol against blackhole attacks in MANET." *International Journal of Engineering and Technology* 2.6 (2010): 444-449.

[11] Zhou Zhi and Yow Kin Choong. Anonymizing geographic ad hoc outing for preserving location privacy. In Distributed Computing Systems Workshops, 2005. 25th IEEE International Conference on, pages 646–651. IEEE, 2005.

[12] Hu, Yih-Chun, David B. Johnson, and Adrian Perrig. "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks." *Ad hoc networks*1.1 (2003): 175-192.

[13] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Ariadne: A secure on-demand routing protocol for ad hoc networks." *Wireless networks* 11.1-2 (2005): 21-38.

[14] Hu, Yih-Chun, and Adrian Perrig. "A survey of secure wireless ad hoc routing."*IEEE Security & Privacy* 2.3 (2004): 28-39.

[15] El Defrawy, Karim, and Gene Tsudik. "Privacy-preserving location-based on-demand routing in MANETs." *Selected Areas in Communications, IEEE Journal on* 29.10 (2011): 1926-1934.

[16] Martin Mauve, A Widmer, and Hannes Hartenstein. A survey on position-based routing in mobile ad hoc networks. Network, IEEE, 15(6):30–39, 2001.

[17] Kwan-Wu Chin, John Judge, Aidan Williams, and Roger Kermode. Implementa- tion experience with manet routing protocols. ACM SIGCOMM Computer Com- munication Review, 32(5):49–59, 2002.

[18] Charles E Perkins and Elizabeth M Royer. on-demand distance vector routing. In Mobile Computing Systems and Applications, 1999. Proceedings. WM- CSA'99. Second IEEE Workshop on, pages 90–100. IEEE, 1999.