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 3, March 2014

An Efficient Secure Aware Reactive Routing Protocol in MANET

Priyanka.M[1,] Velumani.R[2]

Student, Dept. of CSE, K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India

Assistant Professor, Dept. of CSE, K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India

ABSTRACT: The route between source and destination, source identity and destination identity are hide by means of anonymous routing protocols. Anonymous routing protocols use hop by hop encryption or redundant traffic in the existing system, which may cause high cost and it doesn't provide different anonymity protection to source, destination and route. So, we propose a protocol called Anonymous Location Based Efficient Routing Protocol (ALERT). The main technique used to provide anonymity is hierarchical partition. ALERT dynamically partition the network into vertical/horizontal zone. Even though this hierarchical zone partition is used, the security criteria is not satisfied .there may be a chances in node misbehavior .so we propose another concept by trust based node selection. The security rules are generated to select the random node to carry the packet. The security rules consist of logical rules and physical rules. The Greedy perimeter stateless algorithm (GPSR) is used to transmit the data from one node to another. It also effectively avoids the counter intersection attacks and timing attacks. Here we use two rules to securely select the node which relay between source and destination. The two rules are physical and logical rules. NS2 simulation result shows the efficiency of ALERT protocol which used in MANET.

KEYWORDS*:* Anonymous source identity, hop by hop encryption, redundant traffic, routing protocol, GPSR algorithm.

I. INTRODUCTION

Mobile adhoc network (MANET) consists of collection of movable nodes. Adhoc network act as a stand-alone autonomous network. The packet routing is one of the most emerging areas in mobile adhoc network. Research in various aspects of mobile ad hoc networks (MANETs) has been very active, motivated mainly by military, disaster relief, and law enforcement scenarios. More recently, location information has become increasingly available through small and inexpensive GPS receivers, partially prompted by the trend of introducing location-sensing capabilities into personal handheld devices. A natural evolutionary step is to adopt such location-based operation to MANETS. This result in what we term location-based MANETS. In such a MANET, devices rely on location information in their operation. The main distinguishing feature of the envisaged location-based MANET environment is the communication paradigm, based not on permanent or semi-permanent identities, addresses or pseudonyms, but on instantaneous node location. MANETs feature self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. Because of the openness and decentralization features of MANETs, it is usually not desirable to constrain the membership of the nodes in the network. Nodes in MANETs are vulnerable to malicious entities that aim to tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. Although anonymity may not be a requirement in civil oriented applications, it is critical in military applications (e.g., soldier communication). Consider a MANET deployed in a battlefield. Through traffic analysis, enemies may intercept transmitted packets, track our soldiers (i.e., nodes), attack the commander nodes, and block the data Transmission by comprising relay nodes (RN), thus putting us at a tactical disadvantage.

Anonymous routing protocols are essential in MANET to provide anonymity to source destination and route. The attacker utilizes different ways to hack the data between the source and destination also able to find the identity of source and destination. By means of acquiring the direction of the data transmission between source and destination, the attacker can track the correct source and destination. There are different attacks possible in networks.

In order to provide high anonymity protection (for sources, destination, and route) with low cost, we propose an Anonymous Location-based and Efficient Routing protocol (ALERT). ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a no 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 k 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.

II. RELATED WORK

Location Based Routing covers a range of techniques and technologies. A variety of approaches have been proposed to handle GPSR in general and channel load by attacker s in particular. Many approaches leverage physical properties of communications and can be roughly divided into solutions based on location, time, time and location, and network geometry. Other scenarios. In [1], Papadimitratos, et al. give an overview of the problems and challenges associated with GPSR. Their paper includes a set of real-world examples illustrating various threats to neighbor discovery. Location-based solutions offer neighbor discovery protocols to ensure that nodes claiming to be neighbors share the same neighborhood. Coordinated use of both RF and ultrasonic emitters was proposed by Priyantha [2]. Relying on the difference in time of flight between RF and ultrasonic signals, Cricket produces relatively accurate localization both static and mobile nodes at ranges on the order of meters. [3] Uses localized beacons to detect channel load by attacker s while executing a localization protocol for statically deployed nodes. A mechanism for geographically assigning local broadcast keys was used in [4] to limit the range of communications. However, location-based protocols assume the availability of localization information, at least for a subset of participating nodes, making them unsuitable for scenarios without this information A final set of approaches to GPSR relies on properties achievable only in certain contexts. Liu [5] describes GPSR as a problem of neighbor validation and assumes that channel load by attacker capabilities are limited during initial sensor deployment. Nodes securely determine neighbors during this period. Validation is handled through neighbor table exchanges and requires a static and well-connected network. Directional antennas were proposed as a defense against channel load by attacker s in [6]. Although effective, the addition of this type of hardware is limiting and costly in many wireless network deployments. The solution proposed in this article makes use of Multi Dimensional Scaling using oblivious routing (MDSOR) and generic/abstract rigidity and Laman graphs, briefly reviewed as follows. Multidimensional scaling is a class of statistical techniques used to discover relationships in a set of data. The basic idea is that given n objects and a numerical matrix representing inter-object dissimilarities, an equivalent representation of n points in m-dimensional space can be found whose inter-point distances are proportional to the similarities. For 2 dimensions, MDS can reconstruct a complete graph given only the edge lengths. Similarly, MDS can be used to recover coordinates or point configurations from inter-point distances [7]. MDS takes as input an nth matrix of interposing distances, also referred to as a proximity matrix. Laman graphs are sparse graphs describing the minimally rigid systems of rods and joints in a plane. Laman graphs have been studied extensively in rigidity theory. Considering the vertices of a Laman graph in the Euclidean plane, in general, there will be no simultaneous motion of all the points, other than Euclidean congruence's, that preserves the lengths of all the graph edges. It has been shown that the Laman graphs are the minimal graphs with this property [8]. This article extends our earlier work [1], by considering the problem of wormhole localization, and developing a protocol for it. We demonstrate the security properties of our newly developed protocol. Additionally, we further investigate the performance of our proposed secure neighbor discovery protocol, by considering additional factors, such as travel error and localization error. we assume that not all nodes have GPS and/or the environment is GPS-denied (such as in military). In simulation, teams of emergency responders, robots and mobile sensors continuously survey the disaster area. For locating accurately observed events, these mobile entities need to accurate locate themselves, through mobile communication. Consequently, a secure neighbor discovery protocol becomes essential for wireless mobile nodes to correctly obtain their location. Each node is equipped with a single radio transceiver, a ranging capability, and a clock with enough precision to support ranging operations (e.g., hundreds of microsecond’s precision for 0.5–1.5 m ranging accuracy, for acoustic/ ultra-sonic ranging). Communications between nodes use bidirectional symmetric radio transmissions with a range RRF. Ranging radius, RRNG, is similarly bidirectional and symmetric. Nodes are real neighbors if they can communicate via radio and perform ranging operations with each other. Mobile nodes are able to calculate distance traveled with some degree of error (e.g., 2–10% of the distance traveled, using dead-reckoning or simple odometers, e.g., using wheel encoders, human step detection) during ranging operations [9]. The size of the anonymity set may decrease, because nodes are mobile, yet the corresponding anonymity set management is simple. We design techniques to further improve node anonymity and reduce communication overhead. We use analysis and extensive simulation to study the node anonymity and routing performance and to determine the parameters that most impact the anonymity level that can be achieved by our protocol[10].

III. ALERT: AN ANONYMOUS LOCATION-BASED EFFICIENT ROUTING PROTOCOL

A. Networks and Attack Models and Assumptions

ALERT can be applied to different network models with various node movement patterns such as random way point model [17] and group mobility model [18]. Consider a MANET deployed in a large field where geographic routing is used for node communication in order to reduce the communication latency. The location of a message’s sender may be revealed by merely exposing the transmission direction. Therefore, an anonymous communication proto-col that can provide untraceability is needed to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field. Moreover, a malicious observer may try to block the data packets by compromising a number of nodes, intercept the packets on a number of nodes, or even trace back to the sender by detecting the data transmission direction. Therefore, the route should also be undetectable. A malicious observer may also try to detect destination nodes through traffic analysis by launching an intersection attack. Therefore, the destination node also needs the protection of anonymity.

In this work, the attackers can be battery powered nodes that passively receive network packets and detect activities in their vicinity. 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. The assumptions below apply to both inside and outside attackers.

1. Capabilities. By eavesdropping, the adversary nodes can analyze any routing protocol and obtain in-formation about the communication packets in their vicinity 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 vulnerable 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. Incapabilities. The attackers do not issue strong active attacks such as black hole. They can only perform intrusion to a proportion of all nodes. Their computing resources are not unlimited; thus, both symmetric and public/private key cannot be bru-tally decrypted within a reasonable time period. Therefore, encrypted data are secure to a certain degree when the key is not known to the attackers.

B. The ALERT Routing Algorithm

For ease of illustration, we assume the entire network area is generally a rectangle in which nodes are randomly disseminated. The information of the bottom-right and upper left boundary of the network area is configured into each node when it joins in the system. This information enables a node to locate the positions of nodes in the entire area for zone partitions in ALERT.ALERT features a dynamic and unpredictable routing path, which consists of a number of dynamically deter-mined intermediate relay nodes. As shown in the upper part of Fig. 1, given an area, we horizontally partition it into two zones A_1 and A_2. We then vertically partition zone A_1 to B_1 and B_2. After that, we horizontally partition zone B_2 into two zones. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner. We call this partition process hierarchical zone partition. ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message.Fig. 2 shows an example of routing in ALERT.

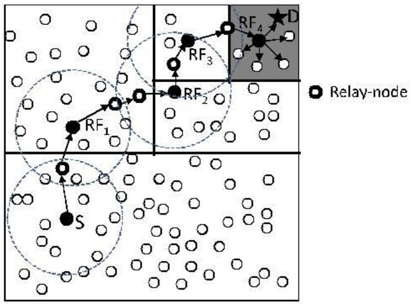


Fig.1. routing among zones in ALERT

We call the zone having k nodes where D resides the destination zone, denoted as Z_D. k is used to control the degree of anonymity protection for the destination process until itself and Z_D are not in the same zone. It then randomly chooses a position in the other zone called temporary destination (TD), and uses the GPSR routing algorithm to send the data to the node closest to TD. This node is defined as a random forwarder (RF). Fig. 3 shows an example where node N_3 is the closest to TD, so it is selected as a RF . ALERT aims at achieving k-anonymity [25] for destination node D, where k is a predefined integer. Thus, in the last step, the data are broadcasted to k nodes in Z_D, providing k-anonymity to the destination.

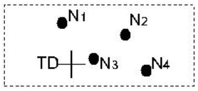


Fig. 3. Choosing a RF according to a given TD.

Given an S-D pair, the partition pattern in ALERT varies depending on the randomly selected TDs and the order of horizontal and vertical division, which provides a better anonymity protection. Fig. 1 shows two possible routing paths for a packet pkt issued by sender S targeting destination D in ALERT. There are also many other possible paths. In the upper routing flow, data source S first horizontally divides the area into two equal-size zones, A_1 and A_2, in order to separate S and Z_D. S then randomly selects the first temporary destination TD_1 in zone A_1 where Z_D resides. Then, S relies on GPSR to send pkt to TD_1. The pkt is forwarded by several relays until reaching a node that cannot find a neighbor closer to TD_1. This node is considered to be the first random-forwarder RF $_1$. After RF $_1$ receives pkt, it vertically divides the region A_1 into regions B_1 and B_2 so that Z_D and itself are separated in two different zones. Then, RF $_1$ randomly selects the next temporary destination TD_2 and uses GPSR to send pkt to TD_2. This process is repeated until a packet receiver finds itself residing in Z_D, i.e., a partitioned zone is Z_D having k nodes. Then, the node broadcasts the pkt to the k nodes. The lower part of Fig. 1 shows another routing path based on a different partition pattern. After S vertically partitions the whole area to separate itself from Z_D, it randomly chooses TD_1 and sends pkt to RF $_1$. RF $_1$ partitions zone A_2 into B_1 and B_2 horizontally and then partitions B_1 into C_1 and C_2 vertically, so that itself and Z_D are separated. Note that RF $_1$ could vertically partition A_2 to separate itself from Z_D in two zones but may choose a TD further away from the destination than the TD that resulted from the horizontal partition. Therefore, ALERT sets the partition in the alternative horizontal and vertical manner in order to ensure that a pkt approaches D in each step.

As GPSR, we assume that the destination node will not move far away from its position during the data transmission, so it can successfully receive the data. In this design, the tradeoff is the anonymity protection degree and transmission delay. A larger number of hierarchies generate more routing hops, which increases anonymity degree but also increases the delay. To ensure the delivery of packets, the destination sends a confirmation to the source upon receiving the packets. If the source has not received the confirmation during a predefined time period, it will resend the packets.

C. The Destination Zone Position

The reason we use Z_D rather than D is to avoid exposure of D. Zone position refers to the upper left and bottom-right coordinates of a zone. One problem is how to find the position of Z_D, which is needed by each packet forwarder to check whether it is separated from the destination after a partition and whether it resides in Z_D. Let H denote the total number of partitions in order to produce Z_D. Using the number of nodes in Z_D (i.e., k), and node density _, H is calculated by

$$H ¼ \log_2 \overline{- - {}^{G}\; ; \, k}$$

where G is the size of the entire network area. Using the calculated H, the size G, the positions ð0; 0Þ and ðx_G; y_GÞ of the entire network area, and the position of D, the source S can calculate the zone position of Z_D. Assume ALERT partitions zone vertically first. After the first vertical partition, the positions of the two generated zones are ð0; 0Þ; ð0:5x_G; y_GÞ and ð0:5x_G; 0Þ; ðx_G; y_G Þ. S then finds the zone where Z_D is located and divides that zone horizon-tally. This recursive process continues until H partitions are completed. The final generated zone is the desired destina-tion zone, and its position can be retrieved accordingly.

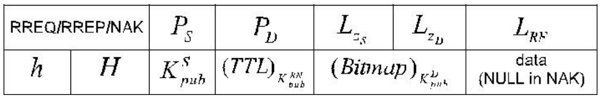
Therefore, the size of the destination zone is example, for a network with size G ¼ 8 and position represented by ð0; 0Þ and ð4; 2Þ, if H ¼ 3 and the destination position is ð0:5; 0:8Þ, the resulting destination zone's position is ð0; 0Þ and ð1; 1Þ with size of $_2{}^8{}_3$ ¼ 1.

D. Packet Format of ALERT

For successful communication between S and D, S and each packet forwarder embeds the following information into the transmitted packet.

1. The zone position of Z_D, i.e., the Hth partitioned zone.
2. The encrypted zone position of the Hth partitioned zone of S using D's public key, which is the destination for data response.
3. The current randomly selected TD for routing.
4. A bit (i.e., 0/1), which is flipped by each RF, indicating the partition direction (horizontal or vertical) of the next RF.

With the encrypted Hth partitioned zone in the informa-tion of (2), an attacker needs very high computation
power to be able to launch attacks such as dictionary attack to



RREQ/RREP/NAK		P_S	P_D	L_{z_S}	L_{z_D}	L_{RF}
h	H	K^S_{pub}	$(TTL)_{K^{RN}_{pub}}$	$(Bitmap)_{K^D_{pub}}$		data (NULL in NAK)

Fig.3. Packet format of ALERT.

decrypt it in order to discover the source S of a session with a specific destination D. Moreover, the Hth partitioned zone is the position of a zone rather than a position, which makes it even harder to locate the source S. Such an attack from an attacker with very high computation power is beyond our practical assumption.

In order to save computing resources, we let the source node calculate the information of (1) and (2) and forward it along the route rather than letting each packet forwarder calculate the values. In order to hide the packet content from adversaries, ALERT employs cryptography. The work in [26] experimentally proved that generally symmetric key cryptography costs hundreds of times less overhead than public key cryptography while achieving the same degree of security protection. Thus, instead of using public key cryptography, ALERT uses symmetric key encryption for transmitted data. Recall that S can get D's public key from the secure location service. In a S-D communication, S first embeds a symmetric key K_s^S , encrypted using D's public key, into a packet. Later, D sends S its requested contents, encrypted with K_s^S , decrypted by its own public key. Therefore, the packets communicated between S and D can be efficiently and securely protected using K_s^S .

Fig. 3 shows the packet format of ALERT, which omits the MAC header. Because of the randomized routing nature in ALERT, we have a universal format for RREQ/RREP/NAK. A node use NAK to acknowledge the loss of packets. The data field of RREQ/RREP is left blank in NAK packets. Flooding-based anonymity routing usually uses ACKs, while NAKs are often adopted in geographic routing-based approaches [13] to reduce traffic cost. For the same purpose, we choose to use NAKs. In the packet, P_S is the pseudonym of a source; P_D is the pseudonym of the destination; L_{ZS} and L_{ZD} are the positions of the Hth partitioned source zone and destination zone, respectively; L_{TD} is the currently selected TD's coordinate; h is the number of divisions so far, H is the maximum allowed number of divisions; and K_s^S denotes the symmetric key of a source. Particularly, ðTTLÞ$_{Kpub}$RN is used for the protection of source anonymity and will be introduced in Section 2.6, and ðBitmapÞ$_{Kpub}$D is used for solving intersec-tion attack and will be discussed in Section 3.3. When node A wants to know the location and public key of another node B, it will contact its location server as described in Section 2.2, thus there is no need to exchange shared keys between nodes.

E. Source Anonymity

ALERT contributes to the achievement of anonymity by restricting a node's view only to its neighbors and constructing the same initial and forwarded messages. This makes it difficult for an intruder to tell if a node is a source or a forwarding node. To strengthen the anonymity protection of the source nodes, we further propose a lightweight mechanism called "notify and go." Its basic idea is to let a number of nodes send out packets at the same time as S in order to hide the source packet among many other packets.

"Notify and go" has two phases: "notify" and "go." In the first "notify" phase, S piggybacks its data transmission notification with periodical update packets to notify its neighbors that it will send out a packet. The packet includes two random back-off time periods, t and t_0. In the "go" phase, S and its neighbors wait for a certain period of randomly chosen time 2 ½t; t þ t_0 & before sending out messages. S's neighbors generate only several bytes of random data just in order to cover the traffic of the source. t should be a small value that does not affect the transmission latency. A long t_0 may lead to a long transmission delay while a short t_0 may result in interference due to many packets being sent out simultaneously. Thus, t_0 should be long enough to minimize interference and balance out the delay between S and S's farthest neighbor in order to prevent any intruder from discriminating S. This camou-flage augments the privacy protection for S by _-anonymity where _ is the number of its neighbors. Therefore, it is difficult for an attacker to analyze traffic to discover S even if it receives the first notification.ALERT utilizes a TTL field in each packet to prevent the packets issued in the first phase from being forwarded in order to reduce excessive traffic. Only the packets of S are assigned a valid TTL, while the covering packets only have a TTL ¼ 0. After S decides the next TD, it forwards the packet to the next relay node, which is its neighbor based on GPSR. To prevent the covering packets from being differentiated from the ones sent by S, S encrypts the TTL field using K_{pub}^{RN} obtained from the periodical "hello" packets between neighbors. Every node that receives a packet but cannot find a valid TTL will try to decrypt the TTL using its own private key. Therefore, only NRN will be able to success-fully decrypt it, while other nodes will drop such a packet.

F. Will Dead End Compromise Anonymity?

Dead end is one common problem in the geographic routing in which each node is aware of the positions of its neighbors in order to forward a packet to the neighbor nearest to the destination. A dead end occurs when a packet is forwarded to a node whose neighbors are all further away from the destination than itself and then the packet is routed between neighbors iteratively. ALERT can incorpo-rate existing solutions [24], [27], [28], such as face routing, to avoid the dead-end problem without compromising anon-ymity protection. In ALERT, the transmission of each packet is based on a series of RFs who decide which region a packet should be sent to. Between any two RFs, the relays perform the GPSR routing. Each relay has no information on the S or D except the destination zone information. Its routing action is based on the coordinate of the next TD. Therefore, relays can incorporate existing solutions to avoid the dead-end problem without exposing any direct infor-mation about the S or D.

IV. ANONYMITY PROTECTION AND STRATEGIES AGAINST ATTACKS

This section discusses the performance of ALERT in providing anonymity protection and its performance and strategies to deal with some attacks.

A. Anonymity Protection

ALERT offers identity and location anonymity of the source and destination, as well as route anonymity. Unlike geographic routing [29], [3], [4], [10], [11], which always takes the shortest path, ALERT makes the route between a S-D pair difficult to discover by randomly and dynamically selecting the relay nodes. The resultant different routes for transmissions between a given S-D pair make it difficult for an intruder to observe a statistical pattern of transmission. This is because the RF set changes due to the random selection of RFs during the transmission of each packet. Even if an adversary detects all the nodes along a route once, this detection does not help it in finding the routes for subsequent transmissions between the same S-D pair.

Additionally, since an RF is only aware of its proceeding node and succeeding node in route, the source and destination nodes cannot be differentiated from other nodes en route. Also, the anonymous path between S and D ensures that nodes on the path do not know where the endpoints are. ALERT strengthens the privacy protection for S and D by the unlinkability of the transmission endpoints and the transmitted data [1]. That is, S and D cannot be associated with the packets in their communica-tion by adversaries. ALERT incorporates the “notify and go” mechanism to prevent an intruder from identifying which node within the source neighborhood has initiated packets. ALERT also provides k-anonymity to destinations by hiding D among k receivers in Z_D. Thus, an eaves-dropper can only obtain information on Z_D, rather than the destination position, from the packets and nodes en route.

The route anonymity due to random relay node selection in ALERT prevents an intruder from intercepting packets or compromising vulnerable nodes en route to issue DoS attacks. In ALERT, the routes between two communicating nodes are constantly changing, so it is difficult for adversaries to predict the route of the next packet for packet interception. Similarly, the communication of two nodes in ALERT cannot be completely stopped by compromising certain nodes because the number of possible participating nodes in each packet transmission is very large due to the dynamic route changes. In contrast, these attacks are easy to perform in geographic routing, since the route between a given S-D pair is unlikely to change for different packet transmissions, and thus, the number of involved nodes is much smaller than in ALERT.

B. Resilience to Timing Attacks

In timing attacks [16], through packet departure and arrival times, an intruder can identify the packets transmitted between S and D, from which it can finally detect S and D. For example, two nodes A and B communicate with each other at an interval of 5 seconds.

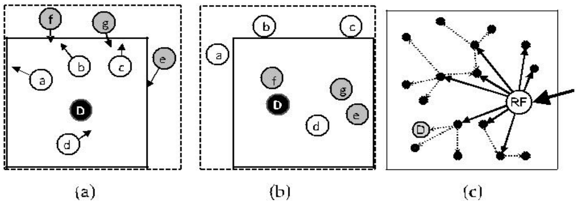


Fig. 4. Intersection attack and solution.

After a long observation time, the intruder finds that A’s packet sending time and B’s packet receiving time have a fixed five second difference such as (19:00:55, 19:01:00) and (20:01:33, 20:01:38). Then, the intruder would suspect that A and B are communicating with each other.

Avoiding the exhibition of interaction between commu-nication nodes is a way to counter timing attacks. In ALERT, the “notify and go” mechanism and the broad-casting in Z_D both put the interaction between S-D into two sets of nodes to obfuscate intruders. More importantly, the routing path between a given S-D and the communication delay (i.e., time stamp) change constantly, which again keeps an intruder from identifying the S and D.

C. Strategy to Counter Intersection Attacks

In an intersection attack, an attacker with information about active users at a given time can determine the sources and destinations that communicate with each other through repeated observations. Intersection attacks are a well-known problem and have not been well resolved [16]. Though ALERT offers k-anonymity to D, an intersection attacker can still identify D from repeated observations of node movement and communication if D always stays in Z_D during a transmission session. This is because as long as D is conducting communication, the attacker can monitor the change of the members in the destination zone containing D. As time elapses and nodes move, all other members may move out of the destination zone except D. As a result, D is identified as the destination because it always appears in the destination zone.Fig. 5a is the status of a Z_D after a packet is broadcasted to the zone. The arrows show the moving directions of nodes. We can see that nodes a, b, c, d, and D are in Z_D. Fig. 5b is the subsequent status of the zone the next time a packet is transmitted between the same S-D pair. This time, nodes d, e, f, g, and D are in Z_D. Since the intersection of the in-zone nodes in both figures includes d and D, D could be identified by the attacker. Therefore, the longer an attacker watches the process, the easier it is to identify the destination node.

To counter the intersection attack, ZAP [13] dynamically enlarges the range of anonymous zones to broadcast the messages or minimizes communication session time. However, the former strategy increases the communication overhead, while the latter may not be suitable for long-duration communication. Instead of adopting such a mitigating mechanism, we propose another strategy to resolve this problem. Note that the attacker can be puzzled and lose the cumulated observation by making it occasion-ally fail to observe D’s reception of packets. Since packets are delivered to Z_D constantly in long-duration sessions rather than using direct local broadcasting in the zone, the last RF multicasts packet pkt_1 to a partial set of nodes.

Fig. 5c shows the two-step process with the first step in solid arrows and the second step in dashed arrows. We can see that 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 pkt_1 and pkt_2 are mixed, an attacker observes that D is not in the recipient set of pkt_1 though D receives pkt_1 in the delivery time of pkt_2. Therefore, the attacker would think that D is not the recipient of every packet in Z_D in the transmission session, thus foiling the intersection attack.

Because the attacker may grab and analyze packets on air, the last forwarding node alters a number of bits in each packet to prevent the attacker from identifying identical packets in one broadcasting. This function is provided by the field ðBitmapÞ$_{Kpub}$D in each packet. The Bitmap records the altered bits and is encrypted using the destination's public key K_{pub}^{D} for recovering the original data. Since destination is not always within the recipient set, and the packet forwarded to a destination is different from the original packet, the attacker cannot identify the destination from its observation history by calculating the intersection set of nodes.

V. CONCLUSION

MANET is an open environment and it is attracted much attention recently. Due to the dynamic nature, MANET prone to different attacks from intruders. To overcome this more number of IDS has been designed. A brief description of different IDS technique to make a secured MANET. Our aim is to reduce the false positives and increase the performance. Most of the detection engines proposed for MANET produce huge amount of false positives. The incorporation of Watchdog/Pathrater with Crosscheck mechanism will reduce overhead as well as increase in throughput. Therefore we believe our proposed IDS will reduce the maximum amount of false positives and overcome the demerits of past methods.

REFERENCES

1. Ashish Kumar, Vidya Kadam, Subodh Kumar, Shital Pawar, "An Acknowledgement – Based Approach for the Detection of Routing Misbehavior in MANETS" International Journal of advances in Embedded Systems, vol.1, Issue.1, 2011.
2. Adnan Nadeem, Michael Howarth, "Protection of MANETs from a range of attacks using an intrusion detection and prevention system", Springer, 2011.
3. Adnan Nadeem, Michael Howarth, "Adaptive Intrusion Detection & Prevention of Denial of Service attacks in MANETs", ACM, 2009.
4. Charlie Obimbo, Liliana Maria Arboled- Cobo "An Intrusion Detection System for MANET" Communications in Information Science and Management Engineering ,vol.2, no.3, 2012.
5. Christoforos Panos, Christos Xenakis, Ioannis Stavrakakis, "A Novel Intrusion Detection System for MANETs", International conference on security and Cryptography, July 2010.
6. Haiying Shen, Member, IEEE, and Lianyu Zhao, Student Member, IEEE "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs" IEEE Transactions on Mobile Computing, Vol. 12, NO. 6, June 2013.
7. Mohammad Wazid, Rajesh Kumar Singh, R.H.Goudar, "A Survey of Attacks Happened at Different Layers of Mobile Ad- Hoc Network & Some available Detection Techniques" IJCA, 2011.
8. Nakayama.H, S.Kurosawa, A.Jamalipour, Y. Nemoto,N.Kato, "Dynamic Anomaly Detect ion Scheme for AODV-Based Mobile Ad Hoc Networks" IEEE Transaction on Vehicular Technology, vol.58, no.5, pp.2471-2481, Jun2009.
9. Prajeet Sharma , Niresh Sharma, Rajdeep Singh, "A Secure Intrusion Detection system against DDOS attack in Wireless Mobile Ad-hoc Network" International Journal of *IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No.5, October 2012* 950 Computer Application, vol.41, no.21, Mar 2012.
10. Pratihari.H.N,"Intrusion Detection System (IDS) for secure MANETs: A Study" International Journal of Engineering Research and Applications, vol.2, Issue.1, pp.962-966, Jan-Feb 2012.
11. Poongodhai, K.Jayarajan, K.Duraiswamy, "A Recent Survey of Intrusion Detection System in Mobile Ad Hoc Networks" International Journal of Communications and Engineering,vol.4, no. 5, Issue.1, Mar 2012.
12. Rajendra V.Boppana, Xu Su, "On the Effectiveness of Monitoring for Intrusion Detection in Mobile Ad Hoc Networks" IEEE Transaction on Mobile Computing,vol.10, no.8, Aug 2011.
13. Rajni Sharma, Alisha saini,"A Study of various Security Attacks & their countermeasures in MANET" IJARCSSE, vol.1, Issue.1, Dec 2011.
14. Sumitra Menaria, Sharada valiveti, Kotecha, "Comparative study of Distributed Intrusion Detection in Ad – hoc Networks" International Journal of Computer Applications, vol.8, no.9, Oct 2010.

15. Saman Desilva, Rajendra V.Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks" IEEE Transaction, 2005.
16. Tiranuch Anantvalee, Je Wu," A Survey on Intrusion Detection in Mobile Ad Hoc Networks" Springer, 2006.
17. Vikas Solomon Abel, "Survey of Attacks on Mobile Ad-Hoc Network" IJCSE ,vol.3, no.2, Feb 2011.
18. Yanqing Zeng, Zhide Chen, Chen Qiao, Li Xu, "A Cluster Header Election Scheme Based on Auction Mechanism for Intrusion Detection in MANET", International Conference on Network Computing and Information Security, 2011.
19. Zhu Ji, Wei Yu, K.J. Ray Liu, "Cooperation Enforcement in Autonomous MANETs under Noise and Imperfect Observation" IEEE SECON, 2006