ISSN 2348 - 7968

IMPROVING THE SECURITY IN MANET USING MRF ALERT PROTOCOL

G.Nithya[1], G.Sujatha[2],

[1]PG Scholar, Applied Electronics, Arunai Engineering College
Tiruvannamalai, India

[2]Assistant Professor, Department of ECE, Arunai Engineering college,
Tiruvannamalai, India

Abstract- Anonymous Location-based Efficient Routing protocol (ALERT) has been proposed to provide full anonymity protection to data sources, destinations, and routes. It has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. ALERT is also resilient to intersection attacks and timing attacks. ALERT dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a nontraceable anonymous route. The analysis of ALERT in terms of anonymity and efficiency is done and also implemented in NS2 to evaluate the performance. In ALERT, the Random Forwarder (RF) node is selected randomly without considering the capacity (Energy level and memory capacity). So there may be a chance of node failure during the transmission. To avoid that, in my project the capacity of the node should be considered while selecting the random forwarder node. To increase the route efficiency, the Random forwarder will be selected by considering the parameter Transmission capability (Power level). In future, the replication attack in the network is detected by using one way hash chain algorithm along with polynomial key.

Index Terms— **Mobile ad hoc networks, anonymity, routing protocol, geographical routing, oneway hash chain algorithm.**

I. INTRODUCTION

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self configuring network of mobile devices connected by wireless links. The Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. It represents complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary, ‘‘ad-hoc’’ network topologies, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure. use of a number of wireless applications on the move. The typical features of the MANETs to act as autonomous entities has resulted in the extensive use of the same in the fields such as commerce, entertainment, education and military services in particular. Another feature that replaces the previous methods is the “Relationship Unobservability” that dissociates the source and the destination providing anonymity for the data transmission path and direction. Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption. The previous methods involved in the generation of anonymity to the nodes are of a higher cost due to the public-key-based encryption and the high traffic generated. This is our main motive to work on a cost efficient implementation of anonymity among the nodes whose performance also is appreciable. Also the previous methods only provide anonymity to the Source and Destination but do not consider the anonymity of the route as illustrated figure.1.

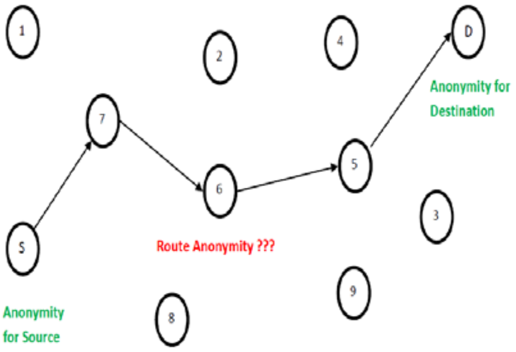


Fig.1Existing Anonymity Providing Methods in MANET

The limited resource is an inherent problem in MANETs, in which each node labours under an energy constraint. MANETs’ complex routing and stringent channel resource constraints impose strict limits on the system capacity. the recent increasing growth of multimedia applications (e.g., video transmission) imposes higher requirement of routing efficiency. However, existing anonymous routing protocols generate a significantly high cost, which exacerbates the resource constraint problem in MANETs. In a MANET employing a high-cost anonymous routing in a battlefield, a low quality of service in voice and video data transmission due to depleted resources may lead to disastrous delay in military operations.

In order to provide high anonymity protection (for sources, destination, and route) with low cost, previously 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 nontraceable 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. ALERT is also resilient to intersection attacks and timing attacks. We theoretically analyzed ALERT in terms of anonymity and efficiency. We also conducted experiments to evaluate the performance of ALERT in comparison with other anonymity and geographic routing protocols. In summary, the contribution of this work includes:

1. Anonymous routing. ALERT provides route anonymity, identity, and location anonymity of source and destination.

2. Low cost. Rather than relying on hop-by-hop encryption and redundant traffic, ALERT mainly uses randomized routing of one message copy to provide anonymity protection.

3. Resilience to intersection attacks and timing attacks. ALERT has a strategy to effectively counter intersection attacks, which have proved to be a tough open issue. ALERT can also avoid timing attacks because of its non fixed routing paths for a source destination pair.

4. Extensive simulations. We conducted comprehensive experiments to evaluate ALERT's performance in comparison with other anonymous protocols.

2. EXISTING METHOD

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

ALERT can be applied to different network models with various node movement patterns such as random way point model and group mobility model. 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 protocol 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.

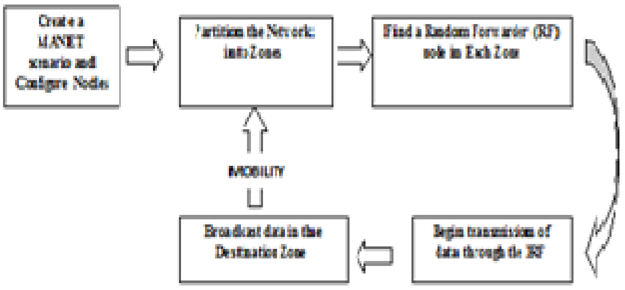

Create a MANET scenario and Configure Nodes
Partition the Network into Zones
Find a Random Forwarder (RF) node in Each Zone
MOBILITY
Broadcast data in the Destination Zone
Begin transmission of data through the RF

Fig.2.Block diagram

1. Capabilities. By eavesdropping, the adversary nodes can analyze any routing protocol and obtain information 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 brutally decrypted within a reasonable time period. Therefore, encrypted data are secure to a certain degree when the key is not known to the attackers.

2.2 Dynamic Pseudonym and Location Service

In one interaction of node communication, a source node S sends a request to a destination node D and the destination responds with data. A transmission session is the time period that S and D interact with each other continuously until they stop. 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, we use a collision resistant hash function, such as SHA-1, to hash a node's MAC address and current time stamp. To prevent an attacker from recomputing the pseudonym, the time stamp should be precise enough (e.g., nanoseconds). Considering the network delay, the attacker needs to compute, e.g., 105, 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 times tamp, we can increase the computation complexity by using randomization for the time stamps. Specifically, we keep the precision of time stamp to a certain extent, say 1 second, and randomize the digits within 1/10th. 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. If pseudonyms are changed too frequently, the routing may get perturbed; and if pseudonyms are changed too infrequently, the adversaries may associate pseudonyms with nodes across pseudonym changes. Therefore, the pseudonym change frequently should be appropriately determined. Each node periodically piggybacks its updated position and pseudonym to "hello" messages, and sends the messages to its neighbours. Also, every node maintains a routing table that keeps its neighbours' pseudonyms associated with their locations.

As previous work, we 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. We can 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, who is aware of the identity of the destination node, to securely obtain the location and public key of the destination node. The public key is used to enable two nodes to securely establish a symmetric key Ks for secure communication. The destination location enables a node to determine the next hop in geographic routing. Specifically, trusted normal nodes or dedicated service provider nodes are used to provide location service. Each node has a location server. When a node A wants to know the location and public key of another node B, it will sign the request containing B's identity using its own identity. Then, the location server of A will return an encrypted position of B and its public key, which can be decrypted by A using the predistributed shared key between A and its location server. When node A moves, it will also periodically update its position to its location server. For high reliability, the location serves can replicate data between each other. Thus, the location servers are allowed to fail, because each node can be in contact with all location servers in range.

We assume that the attacker will not compromise and utilize the location to find out the real identities of nodes that contact with the compromised location server, which is the common assumption of current location services. We leave the work on secure location service as our future. The existence of the location servers are opposed to the ad hoc property of MANETs, and it is not necessary to use location servers in a MANET without security consideration. However, anonymous communication requires third party servers to reliably collect and transmit confidential information, and this solution was used in many of previously proposed works. With the advance of wireless access point (AP), the deployment of location services can be conducted by placing several APs in the whole WIMAX network of civil use at a reasonable cost. It is difficult to preserve all stable location servers in a battle field, but since the location servers are not necessarily be functional all the time and each node only needs to have one usable location server, the location servers can be buried under the ground where anonymous communication is needed.

2.3 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 determined intermediate relay nodes. As shown in the upper part of Fig. 1, given an area, we horizontally partition it into two zones A1 and A2. We then vertically partition zone A1 to B1 and B2. After that, we horizontally partition zone B2 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. We call the zone having k nodes where D resides the destination zone, denoted as ZD. k is used to control the degree of anonymity protection for the destination. The shaded zone in Fig. 3 is the destination zone. Specifically, in the ALERT routing, each data source or forwarder executes the hierarchical zone partition. It first checks whether itself and destination are in the same zone. If so, it divides the zone alternatively in the horizontal and vertical directions. The node repeats this 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).

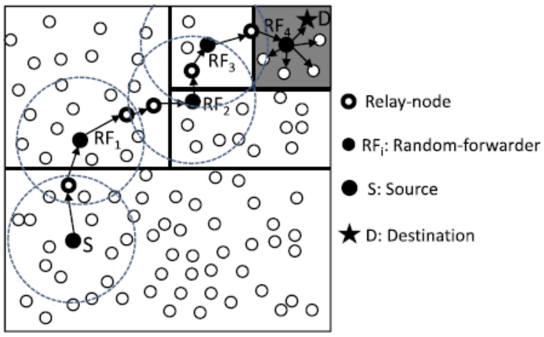


Fig. 3. Routing among zones in ALERT.

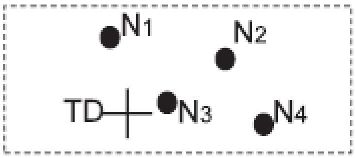


Fig. 4. Choosing a RF according to a given TD.

Fig. 4 shows an example where node N3 is the closest to TD, so it is selected as a RF. ALERT aims at achieving k-anonymity for destination node D, where k is a predefined integer. Thus, in the last step, the data are broadcasted to k nodes in ZD, providing k-anonymity to the destination. 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, A1 and A2, in order to separate S and ZD. S then randomly selects the first temporary destination TD1 in zone A1 where ZD resides. Then, S relies on GPSR to send pkt to TD1. The pkt is forwarded by several relays until reaching a node that cannot find a neighbour closer to TD1. This node is considered to be the first random-forwarder RF1. After RF1 receives pkt, it vertically divides the region A1 into regions B1 and B2 so that ZD and itself are separated in two different zones. Then, RF1 randomly selects the next temporary destination TD2 and uses GPSR to send pkt to TD2. This process is repeated until a packet receiver finds itself residing in ZD, i.e., a partitioned zone is ZD 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 ZD, it randomly chooses TD1 and sends pkt to RF1. RF1 partitions zone A2 into B1 and B2 horizontally and then partitions B1 into C1 and C2 vertically, so that itself and ZD are separated. Note that RF1 could vertically partition A2 to separate itself from ZD 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.

2.4 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 neighbours wait for a certain period of randomly chosen time $\in [t + t_0]$ before sending out messages. k^{RN}_{PUB}S's neighbours 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 neighbour in order to prevent any intruder from discriminating S. This camouflage augments the privacy protection for S by η-anonymity where η is the number of its neighbours. 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= 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^{RN}_{PUB} obtained from the periodical "hello" packets between neighbours. 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 successfully decrypt it, while other nodes will drop such a packet.

3. 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.

3.1 Anonymity Protection

ALERT offers identity and location anonymity of the source and destination, as well as route anonymity. Unlike geographic routing, 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 . That is, S and D cannot be associated with the packets in their communication 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 ZD. Thus, an eavesdropper can only obtain information on ZD, 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.

3.2 Resilience to Timing Attacks

In timing attacks, 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. 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 communication nodes is a way to counter timing attacks. In ALERT, the "notify and go" mechanism and the broadcasting 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.

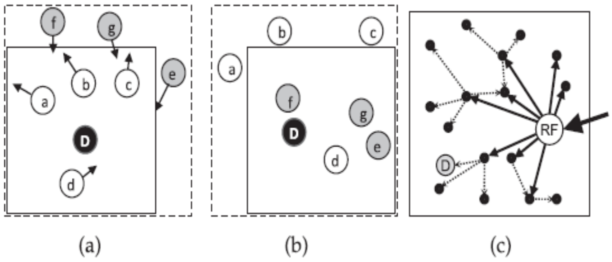


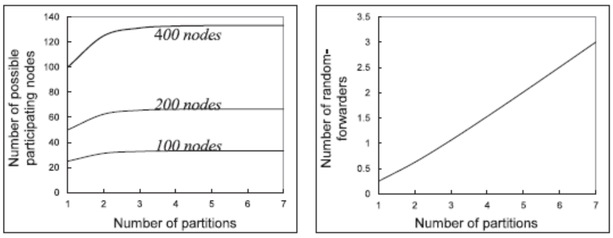
Fig. 5. Intersection attack and solution.

3.3 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 . 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 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 occasionally 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 pkt1 to a partial set of nodes, say m nodes out of the total k nodes in the zone. The m nodes hold the packets until the arrival of the next packet pkt2. Upon the arrival of the next packet, the m nodes conduct one-hop broadcasting to enable other nodes in the zone to also receive the packet in order to hide D. 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 pkt1 and pkt2 are mixed, an 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 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 (Bitmap) 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. This approach incurs two extra costs. One is the one hop broadcasting of the recipients in the destination zone. The other is the encryption cost of changed bits.

The Number of Possible Participating Nodes:

The intention of this analysis is to characterize how many possible nodes are able to participate in one S-D routing. The number of these nodes shows how many nodes can become camouflages in a routing path. These possible participating nodes include RFs and the relay nodes between two RFs using GPSR. The nodes that actually conduct the routing are not easily discovered among the many possible participating nodes, thus making the routing pattern undetectable. Because the positions of both S and D affect the number of possible participating nodes in routing, the positions influence routing anonymity.



(a) Estimated possible participat- (b) Estimated random-forwarders.

Fig 6.Estimated routing nodes

We first calculate the probability that σ partitions are needed to separate S and D denoted as $\rho_s(\sigma)$. We use σ to denote the closeness between S and D. $\rho_s(\sigma$ actually is the probability that D is located in a position that can be separated from a given S using σ partitions. We can get

$$\rho_s(\sigma) = \frac{1}{2^\sigma} \text{ ,}0 < \sigma \leq \text{H}\ldots\ldots\ldots\ldots\ldots \qquad 1$$

We use Ne(σ) to denote the expected number of nodes that possibly take part in routing based on a given closeness σ:

$$\text{Ne}(\sigma)\text{=}a(\sigma, l_A)b(\sigma, l_B)\rho\ldots\ldots\ldots\ldots\ldots \qquad 2$$

where ρ denotes the density of nodes. By considering different closeness σ, we arrive at the final expected number of possible participating nodes from a S to any D:

$$N_e\text{=}\sum_{\sigma=1}^{H} N_e(\sigma)\rho_s(\sigma)\text{=}\sum_{\sigma=1}^{H}(a(\sigma, l_A)\, b(\sigma, l_B)\rho)\frac{1}{2^\sigma}\ldots\ldots\ldots\ldots \qquad 3$$

4.One way hash chain algorithm:

One-way chains are an important cryptographic primitive in many security applications. As one-way chains are very efficient to verify, they recently became increasingly popular for designing security protocols for resource-constrained mobile devices and sensor networks, as their low-powered processors can compute a one-way function within milliseconds, but would require tens of seconds or up to minutes to generate or verify a traditional digital signature. Recent sensor network security protocols thus extensively use one-way chains to design protocols that scale down to resource-constrained sensors. A one-way function is a function that is easy to compute on every input, but hard to invert given the image of a random input. Here "easy" and "hard" are to be understood in the sense of computational complexity theory, specifically the theory of polynomial time problems. Not being one-to-one is not considered sufficient of a function for it to be called one-way hash chain is the successive application of a cryptography hic hash function to a piece of data. In computer security, a hash chain is a method to produce many one-time keys from a single key or password. For non-repudiation a hash function can be applied successively to additional pieces of data in order to record the chronology of data's existence. A hash chain is a successive application of a cryptographic hash function to a string. For example,

$$h(h\left(h(h(x))\right))$$

gives a hash chain of length 4, often denoted.

One of the important fundamental problems in cryptography is a Polynomial Reconstruction Problem (PRP). There are several public key cryptographic systems constructed based on this problem. This paper provides an analytical study on a public key cryptosystem (*PKC*) that is based on bivariate polynomial Reconstruction Problem (*BPRP*) and takes into considerations the developments performed on the (*PKC*). A modification is proposed using bivariate polynomial instead of univariate polynomial which is used in the original Augot's system to enhance its security. The analysis concerned mainly the mathematical backgrounds related to bivariate polynomials and the operation, valid generally for these polynomials, especially in the finite fields *GF*(*q*). The coding problem is included in the public key cryptosystem that considers the (*BPRP*). The Reed-Solomon Code is used in such type of (*PKC*) based on (*BPRP*).

Cryptographic system based on bprp:

Augot and Finiasz (2003) proposed the first public key encryption scheme based on the (PRP). This section will present discussion of the performances and state the parameters that are required to reach the desired security level from such scheme. Let us consider the following parameters:

- Fq is a finite field, *q* is the size of *Fq*.

- n is the length of the Reed –Solomon code used by this scheme.

- k its dimension.

believed to be hard, or it must have *W* >(*n* - *k*) / 2 which need to be verified.

- *w* is the weight of a small error *e*, such that *w* ≤(*n* - *k*) / 2

Key Generation Process

Let us consider that we have two parties *A* and *B*. Then want to have their communication using modified cryptosystem based on the bivariate polynomial.

A secretly does the followings:

- Choose the sets *x* and *y*.

- Generates a monic (unitary) bivariate polynomial *p*(*x*, *y*) of degree equal to *k* -1, with respect *x* and of degree equal to *k*-1 with respect *y*.

- Generates an error vector *E* of dimension *n* with the weight *W*, where *W* is exactly non zero coordinates.

- Computes the codeword $C = ev(\ p(X, Y)) = p(xi\ , yj\ )$ of RS_k , ∃ $xi = I$ and $j\ y = j$ for $i = 1,2,\ldots\ldots.,n$ and $j = 1,2,\ldots\ldots.,n$.

- Computes $Pk = C + E$,

where *Pk* is the public-key, while *C* and *E* are kept secret or the secret-key is (*C, E*).

Encryption Process

Let us consider that B wishes to send a message to A. The message

m_0 of length *k* +1 over the alphabet F_q. The following steps will be performed:

- Generates the m_o bivariate polynomial of length *k* +1, where m_0=$m_{0,0}$,................,$m_{0,k+1}$is seen as the polynomial :

m_0(X,Y)=$m_{0,0}$+$m_{0,1}$Y+$m_{0,2}$X+……..+$m_{0,k-2}X^{k-2}Y^{K-2}$

- The message is firstly encoded using (Reed-Solomon Code) into a codeword *m* in *RSk-1*.

- Randomly generates a primitive element $\alpha \in F_q$.

- Randomly generates an error pattern vector *e* of dimension *n* with the weight *w*, where *w* is exactly nonzero coordinates.

- Compute the cipher text

$CT = m + \alpha \times Pk + e$.

Decryption Process

We proposed a modification to this system by using Vander monde interpolation Method instead of Berlekamp-Welch Interpolation that was used in the original Augot system. Hence we will describe the steps of the proposed decryption process. Upon receipt of

$$CT = m + \alpha\times Pk + e.$$

A will perform the following steps:

- Considers only the positions where *E* i = 0.

- Considers the shortened code of length *n-W* which is also a Reed Solomon Code of dimension *k*, ( ) *k RS* .

- Solve the equation $\overline{m}$ +α ×$\bar{C}$ +$\bar{e}$ = $\overline{CT}$,

where *m* , *C* , *e* correspond to the shortened versions of$\overline{m}$, $\bar{C}$, $\bar{e}$. And *E* has disappeared, $\overline{m}$ +α ×$\bar{C}$ ∈ $\overline{RS}$

Computes by using Vander monde interpolation Method, the unique polynomial *q*(*X, Y*) of degree *k* -1 such that *ev*(*q*(*X,Y*)) = $m\overline{m}$+α ×$\bar{C}$.

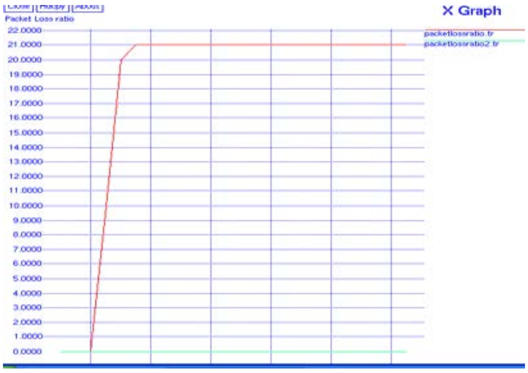
- Computes 0 $q(X ,Y) - \alpha\ p(X ,Y) = m\ (X ,Y)$, where *α* leading coefficient of *q*(*X, Y*), $\bar{C}$ = *ev*(*p*(*X, Y*)) and *p*(*x, y*) has degree 0 *k* −1,deg(*m*) ≤ *k* − 2.

4. Security implications

In our modified scheme based on bivariate polynomial, we have managed to apply the scheme on key generation process, encryption and decryption processes of the cryptosystem. This improvement has increased the security level compared with the original cryptosystem which was based on a univarate polynomial. The adversaries will have to solve for two variables equation systems instead of just a single variable in the univarate version. This in return will give more running time to attack the bivariate polynomial cryptosystem based.

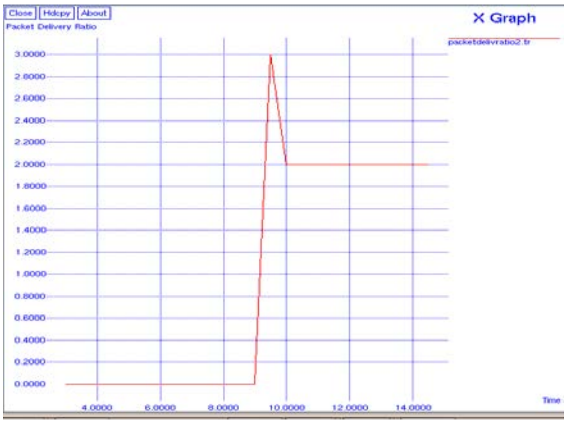
SIMULATION RESULT

Packet loss:



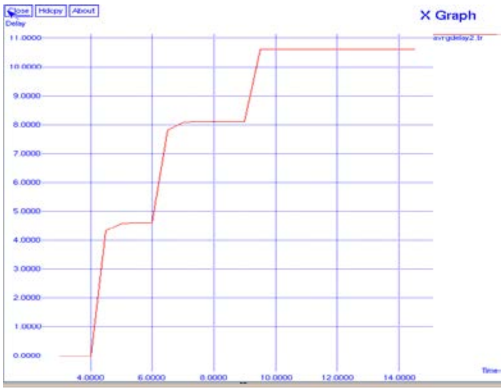
Packet delivery ratio:

This shows the packet delivery ratio is high compare to existing methods.

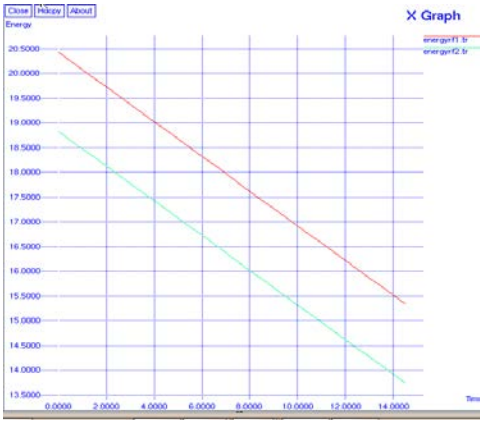


DELAY

This result show the packet delay is very less compared to other methods.



ENERGY vs TIME



CONCLUSION

ALERT is distinguished by its low cost and anonymity protection for sources, destinations, and routes. It uses dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. ALERT further strengthens the anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators receivers. It has the "notify and go" mechanism for source anonymity, and uses local broadcasting for destination anonymity. In addition, ALERT has an efficient solution to counter intersection attacks. ALERT's ability to fight against timing attacks is also analyzed. Experiment results show that ALERT can offer high anonymity protection at a low cost when compared to other anonymity algorithms. It can also achieve comparable routing efficiency to the base-line GPSR algorithm. In this paper to consider the Random forwarder node replication attack. To consider this attack, set up server going to assigns the key for each random forwarder node. The key is generated by using the polynomial bivariate key generation scheme. The key wrapping algorithm is used to protect the key from the adversary.

ACKNOWLEDGEMENT

I like to express heart full thanks to Mrs.G.Sujatha, assistant Professor, Department of ECE, to spend his valuable time to do this project and also I want to thank to my college and my friends for their support.

REFERENCE

[1] A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, "Anonymity,Unlinkability, Unobservability, Pseudonymity, and Identity Managementa Consolidated Proposal for Terminology, Version 0.31,"technical report, 2005.

[2] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "AnAnonymous On-Demand Position-Based Routing in MobileAd Hoc Networks," Proc. Int'l Symp. Applications on InternetSAINT), 2006.

[3] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad HocRouting for Preserving Location Privacy," Proc. Third Int'l WorkshopMobile Distributed Computing (ICDCSW), 2005.

[4] V. Pathak, D. Yao, and L. Iftode, "Securing Location AwareServices over VANET Using Geographical Secure Path Routing,"Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008.

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

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

[7] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," WirelessNetworks, vol. 11, pp. 21-38, 2005.

[8] I. Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for StrongAnonymity in Ad Hoc Networks," Proc. Securecomm and Workshops,2006.

[9] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, "An EfficientAnonymous Communication Protocol for Peer-to-Peer Applicationsover Mobile Ad-Hoc Networks," IEEE J. Selected Areas inComm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[10] X. Wu, "AO2P: Ad Hoc On-Demand Position-Based PrivateRouting Protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4,pp. 335-348, July/Aug. 2005.