International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015) pp 34328-34334

MPKGRP: Mobility prediction and N-Anonymity based geographical routing protocol

[1]T.Sarathamani, [2]Dr. M. Rajesh Babu
[1]Assistant Professor, Department of Computer Science and Engineering, Dr. G. R. Damodaran college of Science, Coimbatore
[2]Professor, Department of CSE, Karpagam College of Engineering, Coimbatore.

Abstract- Nodes in MANETs are not resistant proof because adversary or intruder tampers, analyzes traffic pattern and destination identities through sniffing. It tends to attack the routing protocol and packet transmission in a network. This work proposes a novel protocol called MPKGRP (Mobility prediction and N-Anonymity based geographical routing protocol) improves the update node's position by dynamic Location Update and enhance security by N-anonymity and cryptography. Dynamic Location Update (DLU) is used to predict the mobility of nodes. DLU employs Simple Mobility Prediction model (MP) model for mobility prediction. This model helps sender to identify whether relay node or forwarder is in communication area or not. It overcomes the packet loss and transmission delay by knowing link breakage earlier. The sender uses this location information for sending the packet to destination through the forwarder in network. N-Anonymity based routing protocol hides packet transmission direction and destination node from adversary. Blowfish algorithm is employed in this work to ensure secure communication and packet protection. In experimental analysis, proposed methodology provides better results in terms of low average delay, energy, beacon overhead and neighbor ratio with higher PDR value.

Keywords- Blowfish algorithm, Dynamic Location Update, geographical routing protocol, mobility prediction, N-Anonymity

1. Introduction

Wireless networking is a technology that enables communication between two or more computers using standard network protocols through wireless medium. Primarily, wireless model consists of a large number of Mobile Nodes (MNs) and relatively fewer, but more powerful and fixed nodes. The communication between a fixed node and a MN within its range occurs using the wireless medium. Therefore, it requires fixed permanent infrastructure. Mobile Ad-hoc NETwork (MANET) is a system model which contains a self-organizing collection of MNs used to form a temporary and dynamic wireless network on a shared wireless channel without the aid of a fixed networking infrastructure or centralized administration [1, 2]. Mobile Ad-hoc NET work is widely used because of its mobile nature. It is flexibly deployed in many areas (e.g., conference rooms, forests, battlefields, military, etc.) without the need of any fixed network or centralized administration. Each node serves as a router and executes mobility functionalities in an autonomous manner.

Due to the open transmission medium and decentralization of mobile network, nodes are resistless to malicious activities that may try to alter and examine data and traffic by communication snooping or attack the routing protocols. Through snooping, adversary can capture transmitted packets, track nodes, hit the head nodes and stop the data transmission by compromising relay nodes (RN).

The adversary knows node identities and analyzes the traffic by compromising intermediate nodes which tends to affect routing protocol. To overcome these types of attacks, anonymity is needed. Anonymity in MANETs includes identity and location anonymity of senders and destinations, as well as route anonymity. In order to hide the relationship between source and destination [3], necessary anonymous path between the source and destination is required. It makes that no nodes in network have knowledge between two endpoints location. Present anonymity routing protocols have two main classes: hop-by-hop encryption [4-8] and redundant traffic [9-15].

It has several drawbacks: spotlight on problem for implementing anonymity because public-key-based encryption and high traffic produces high cost. Most of approaches don't offer anonymity protections [4] [15]. Many anonymity routing algorithms [3-6], [10, 11], [13] are based on the Greedy Perimeter Stateless Routing (GPSR) [16], which helps to forward a packet to the node closest to the destination greedily. Strict relay node selection exposes the source and destination and analyzes traffic easily in this routing protocol.

Due to minimum resources constraint in MANET, battlefield uses high-cost anonymous routing, a low quality voice and video data transmission which cause the catastrophe postponement in military operations. In addition, a rapid growth of multimedia applications forces to increase the necessity of routing efficiency.

This paper focuses on low cost N-anonymity routing protocol and mobility prediction which is based on zone partition method and simple linear motion. This prediction is used to adjust the frequency of beacon generation, when the nodes change their motion characteristics. The beacons contain motion characteristics which broadcast to a node's neighbors, where neighbors track the node's motion using simple linear motion. It helps to identify the node's coverage area. In order to protect the destination node and packet transmission direction, N-Anonymity Routing Protocol is used. For secure packet content transmission and zone position from adversaries, cryptography is utilized.

This paper is organized as follows: Section 2 gives various related work towards this technique implemented by

different authors. In Section 3 and 4, network and threat model and proposed technique is briefly explained and in Section 5, the performance of this technique is evaluated using existing technique with some performance metrics and finally Section 6 provides conclusion of this work.

2. Related work

Heissenbuttel et al in 2007 [17] says that in highly mobile ad-hoc networks, periodic beaconing can cause the inaccurate local topologies, which leads to performances degradation, e.g., frequent packet loss and longer delay. The authors say that outdated entries in the neighbor list are the major source that decreases the performance. The proposed optimization technique adapt beacon interval to node mobility or traffic load, including Distance-Based beaconing, speed-based beaconing and reactive beaconing.

The geographic routing protocols such as IGF [18], GeRaf [19], BLR [20], and ALBA-R [21] do not need to maintain the neighbor list and avoid position updates are referred as beaconless routing protocols. Here, the forwarding node broadcasts the data packet to all its neighbors and packets relay on the nodes are desired by the distributer. In these protocols, usually after receiving a packet, each neighbor sets a timer for relaying the packet based on some metrics like the distance to the destination. The beaconless routing protocols avoids excessive position updates and are most suitable for networks, where the topology is highly dynamic by the neighbor nodes which has least timer to expire initially. Then on overhearing the relayed packets, other nodes can cancel their timers and by that duplicate packets are not transmitted [22].

Efficient Geographic Multicast Protocol (EGMP) is a geographic routing which has higher packet delivery ratio when compared with Greedy Perimeter Stateless Routing (GPSR). This is based on greedy forwarding technique, where nodes have only local knowledge of neighbor's position, energy levels and the location of the destination. Based on certain threshold, forwarding decision is made by distance calculations and energy levels. With the highest energy level, the packet is forwarded to the neighbor closest to destination and by adjusting the transmission power. The objective of the algorithm is to prolong the lifetime of the sensors and hence the network lifetime. This protocol is scalable and conserves more energy than other topology based protocols. This algorithm performs better in energy consumption and there is a performance gain in network lifetime. One of the drawbacks of this algorithm is that it suffers from diffusion whole problem [23].

Network Geographic and Energy Aware Routing (GEAR) protocol assumes localization system and targets life time which follows flat routing protocol. It consists of two forwarding phases: forwarding the packet towards a targeted region and disseminating the information within that region. Based on distance to destination it routes packets. Each node maintains an estimated and a learned cost value for each destination. The learned cost value is used for forwarding the packets to nodes which are far away from destination, to avoid holes in the network. Next dissemination stage is based either of recursive geographic forwarding for dense networks or flooding in sparse networks [24].

3. Network and threat model

Network model

Mobile Ad hoc Network is built of several nodes, which uses a dynamic pseudonym as its node identifier. Links between the nodes are taken as bidirectional and beacons are used to update the current location and velocity of the nodes. Hence, each node is aware of their own position and velocity. MPKGRP protocol is used as routing protocol in this work and mostly employed in various network models. Each model has different pattern of node movement like random way point, group mobility model, etc. A MANET is used in different areas of domains, where node communication mainly depends on geographic routing because of reducing the communication delay. The location of a sender can be identified by their transmission direction. Hence, an anonymous communication protocol provides inability to discover the message sender where it follows anonymity, when the sender communicates with the other side of the field. The network uses identity-based public key system for data protection during packet transmission.

Threat model

Nodes in the network are not resistant proof. An active adversary may compromise nodes and use those nodes to create attacks in MANET. An adversary can block or intercept the data packets by compromising a number of nodes or identify the data transmission direction by tracing back to the sender. Hence, the routing direction of packet is also detectable. An adversary can find the destination nodes by analyzing traffic through the intersection attack. Hence, the destination node is in need of anonymity protection.

4. Proposed Methodology

MANET environment consist of nodes in which each node follows geographic routing protocol. Links between the nodes are taken as bidirectional and beacons are used to update the current location and velocity of the nodes. Due to the mobility nature, velocity and position of node may change frequently which cause link failure. In this paper, the dynamic Location Update is used to calculate the node position with the help of Mobility Prediction (MP) model. This model utilizes the simple mobility prediction scheme. Each node knows its velocity and position. This model is used to predict whether node is in communication area or not. Hence, nodes are aware of their link breakage earlier. The sender uses this location information for sending the packet to destination in the network. The adversary easily attacks the packet transmission using sniffing attack by knowing sender transmission direction of packet. N-Anonymity based routing protocol and blowfish cryptographic algorithm is used to enhance the packet transmission.

MPKGRP PROTOCOL

Dynamic location Update

Position update methods deployed in MANET nodes involves more cost, consumes energy, bandwidth, and increases packet collision at the medium access control layer. Due to packet collision and minimized accuracy, the present local topology causes packet loss, degrades routing performance and increased end-to-end delay. Moreover, nodes often differ in

their mobility behavior such as speed, direction, etc. Hence, it requires position update beacon frequently. Most of the nodes do not provide dynamism frequently, small number of nodes contributes in forwarding the packet, but nodes which are located far away from the forwarding path also employs update beacon. This type of periodic broadcasting of beacons is not useful. Dynamic Location Update (DLU) eliminates the drawbacks of periodic beaconing by adapting to the system variations. DLU is used in geographic routing, which dynamically updates the position based on the mobility dynamics of the nodes and forwarding patterns in the network.

Mobility Prediction model

Mobility Prediction model is used to adjust the frequency of beacon generation, when the nodes change their motion characteristics. The beacons contain motion characteristics which broadcast to a node's neighbors where neighbors track the node's motion using simple linear motion. Some nodes in network change their motion in the network frequently. They have to change their position frequently with its neighbors. Few nodes change their motion slowly, their position updates with its neighbor is not needed frequently. This update doesn't fulfill the needs at the time, because the update interval for slow and fast mobile nodes causes useless and inaccurate position information. To solve the above problem, the Mobility Prediction scheme is proposed. After receiving update from a node j, its neighboring nodes changes $j's$ position and velocity information in their table by track node $x's$ location and check whether node j is within the transmission range using simple prediction scheme based on linear kinematics at the period of time. The next beacon is received from node j, when error between the predicted location in the neighbors of node j and node $j's$ actual location is greater than threshold.

When nodes are in a 2D coordinate system, the location is defined by $x\ and\ y$ coordinates. In 3D coordinate system, velocity is along with $x\ and\ y$ coordinates at time T_e. Hence, current position of j^{th} node with respect to the neighbor node can be calculated as follows,

$$X_a^j = X_h^j + (T_l - T_e) * V_x^j$$

$$Y_a^j = Y_h^j + (T_l - T_e) * V_y^j$$

Where (X_h^j, Y_h^j) and (V_x^j, V_y^j) are the location and velocity of node j at time T_e. T_e Specifies the last beacon broadcast and T_c is the current time. The node j uses the same prediction scheme to record its predicted location from its neighbors. The actual location of node n, is denoted by (X_a, Y_a). The deviation is calculated by

$$D_{dev}^j = \sqrt{(X_a^j - X_h^j)^2 + (Y_a^j - Y_h^j)^2}$$

If D_{dev}^j is greater than threshold, its current location and velocity of node j is transmitted as a new beacon. This scheme helps to know current position of nodes in the network and thus reduce the packet loss.

N-Anonymity Routing Protocol

An adversary can block or intercept the data packets by compromising a number of nodes or identify the data transmission direction by tracing back to the sender. Hence, the routing direction packet is also detectable. An adversary can find the destination nodes by analyzing traffic through the intersection attack. Hence, the destination node is in need of anonymity protection. In order to protect the destination node and packet transmission direction, N-Anonymity Routing Protocol is used.

In this protocol, network area is considered as rectangle, where nodes are randomly distributed. The node in rectangular area contains the detail about bottom-right and upper left boundary of the network area and this information helps to locate the node in area for partition. It consists of adaptively known intermediate relay node's location and velocity using mobility prediction which is described in the previous section. It has dynamic and unpredictable routing path.

The area Z is horizontally divided into regions (zones) of $Z_1$and Z_2 and vertically divides the region Z_1 into $Y_1$and Y_2. Further, horizontally divides Y_1 region into two regions. The region partitioning consecutively occurs in an alternating horizontal and vertical manner. This process is referred as hierarchical region partition. Next, select node in region as a relay node based on mobility prediction. This node is used to create an unpredictable routing path for a message. Region has number of nodes n, where destination node D resides in a zone, denoted as Z_D and n is degree of anonymity protection for the destination node. Each relay node starts hierarchical zone partition, and checks whether the destination and source are in same zone. If both nodes are present in the same zone, horizontal and vertical partition is done consecutively. If not, the relay node randomly chooses the position in the next zone called temporary destination (TD), send the data to node which is closest to TD node using mobility prediction and shortest path algorithm (A* algorithm[25]). This node is defined as random forwarder (RF). This routing aims at N-Anonymity for destination node D. The partition pattern changes according to the randomly chosen TDs and the degree of horizontal and vertical partition which gives high anonymity protection.

Location of Destination Zone

Upper left and bottom-right coordinates of a zone is called zone position. It is needed to find out the position of Z_D, where it requires by each forwarder to find whether it is isolated from the destination after a division or resides in Z_D. The total number of zone divisions are denoted as H. Number of nodes in Z_D and the node density ρ, H can be computed as

$$H = \log_2(\frac{\rho.G}{n})$$

Where G is denoted as size of entire network area and the zone position Z_D is calculated by H, size of G, position (0, 0) and (x_G, y_G) of entire network area, position D and source S. This recursive process continues until H partitions are completed. The final generated zone is the desired destination zone, and its position can be retrieved accordingly. Therefore, the size of the destination zone is $\frac{G}{2^H}$.

Packet Format

The packet from source to destination is successfully transferred by each relay nodes embeds the following details into the transmitted packet.

1. The zone position of Z_D.
2. The encrypted zone position of total zone partitioned (H) of Source using D's public key.
3. The dynamically chosen TD currently for forwarding.
4. Binary bit (0/1) is flipped by each random forwarder, indicating the partition direction of the next random forwarder.

The encryption zone position and packet content is done by Blowfish Cryptographic Algorithm.

Due to the randomized routing, each node use Negative acknowledgement (NAK) format to acknowledge the loss of packets and reduce traffic cost, where the field of RREQ/RREP is empty in NAK packets. In all the packets, S and D is the pseudonym of a source and destination, P_{Z_S}, P_{Z_D} and $P_{TD}$are the positions of the H-th partitioned source zone, destination zone and currently selected TD's coordinate, x is the number of partitions so far, H is the total number of allowed divisions, k_s denotes the symmetric key of a source , $(Time\_to\_live)_{n_{pub}^{RN}}$ for the protection of source anonymity and $(Bitmap)_{n_{pub}^{D}}$ is to prevent intersection attack. The RN denotes relay nodes.

Cryptography

For secure packet content transmission and zone position from adversaries, cryptography is utilized. Cryptography gives a number of security goals to ensure the privacy of data, non alteration of data and so on. Because of its wide merits, it is used in many applications. Encryption is done in two ways of method: symmetric key and asymmetric key algorithm. It usually uses symmetric based encryption algorithm. This blowfish encryption is a symmetric key algorithm and it is used here for secure packet communication.

Blowfish is a type of variable-length key, 64-bit block cipher. This algorithm consists of two parts: a key expansion part and a data- encryption part. Key expansion converts a key of at most 448 bits into several sub-key arrays totaling 4168 bytes. Data encryption occurs via a 16-round Feistel network [27]. Each round consists of a key dependent permutation, a key and data-dependent substitution. All operations are X-ORs and additions on 32-bit words.

Source Anonymity

To maximize the anonymity protection, "notify and go" techniques are used. The nodes transfer packets simultaneously. These nodes act as source node to hide the source packet among other packets.

In "notify" phase, source S send periodical update packets to its neighbors that contains data transmission notification to transfer a packet. The transferred packet contains two random time periods, t and t_0. In the "go" phase, before sending out messages, source and its neighbors stand by period of dynamically selected time [t, t+ t_0]. S's neighbors generate bytes of random data just in order to cover the traffic of the source. If rand (t) is minimum time period, transmission latency will neglect. A long t_0 causes long transmission delay whereas short t_0 cause small interference. Hence, t_0 is in long value that reduces interference and reduce the delay between source and source's farthest neighbor. Thus, it prevents any adversary from identifying the source.

Time To Live (TTL) field is used to minimize the traffic by blocking the packets generated in the first phase from being transferred. The valid TTL is in source packets, where false packets have a TTL=0. After selecting the next TD by source, it sends packet to the next forwarder based on mobility prediction and A* algorithm. To stop identify the false packets from source packet; source node encrypts the TTL field using n_{pub}^{RN} periodical "hello" packets between neighbors. Destination Node receives a packet cannot identify the valid TTL by decrypt the TTL using its own private key. Next relay node (NRN) successfully decrypt it, where other nodes will lose the packet.

5. Performance Analysis

In the experimental analysis, analyze the anonymity and routing efficiency properties of MPKGRP and its performance are analyzed using proposed methodology. The proposed methodology is implemented using NS-2. It is popular and well known network simulator tool. This tool is used in the area of MANET, wireless sensor network, etc. In this work, the network consists of 50 mobiles nodes and attacker node. The simulation model of network is given figure 1.

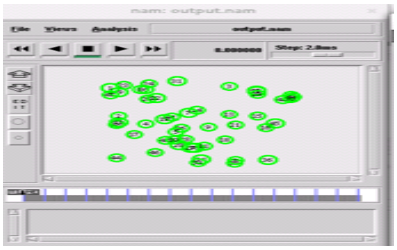

Fig 1: Simulation model of network

The simulation parameters are used while implementing this proposed technique, which is summarized below in the Table 1. These parameters are used for constructing the network. ALERT protocol [26]is taken as existing work and compared with proposed MPKGRP protocol.

Table 1.Simulation Parameters

Simulation Parameter	**Value**
Propagation	Two Ray Ground
Channel	Wireless Channel
Physical Layer	Wireless Physical
Queue	Drop Tail / Pri Queue
Mac	802_.11
X dimension of the topography	500
Y dimension of the topography	500
Ad hoc Routing	AODV
Antenna	Omni Antenna
Max packet	100
Number of nodes simulated	50
Cp	./cbr
Sc	nodes50
Simulation time	100 s
Energy	Energy Model
Initial Energy	100
Min Neighbor	6
Security Duration	4
Adversary node	5

Simulation Parameters

Evaluation metrics

The performance of this work is measured using the beacon overhead, packet delivery ratio, energy, overhead delay, average delay and Neighborhood ratio which shows its efficient result towards the MPKGRP protocol. These results are discussed briefly below.

Beacon Overhead

Overhead - It is the ratio of total number of control packets generated to the total number of data packets received during the simulation time given in equation (1).

$$overhead = \frac{data\ packets\ received}{control\ packets\ generated}$$

The Figure 2 shows the beacon overhead graph for ALERT and MPKGRP. Figure 2 shows that ALERT has high Beacon Overhead value whereas proposed MPKGRP take lesser beacon.

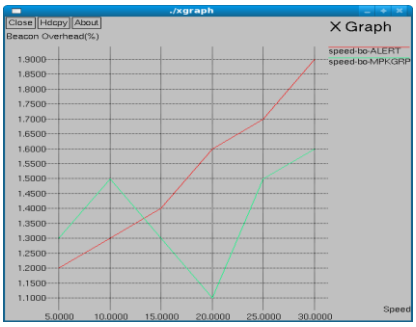

Fig 2: Comparison Graph for Beacon Overhead

Energy

Energy - The percentage of energy consumed by a node is calculated as the energy consumed to the initial energy. Energy consumed by all the nodes in a scenario can be calculated as the sum of individual energy consumption of the nodes by the number of nodes as defined in equation.

$$Average\ Energy\ Consumed = \frac{Sum\ of\ Percent\ Energy\ Consumed\ by\ all\ nodes}{Number\ of\ Nodes} * \text{joule}$$

The Figure 3 shows the graph of energy required for ALERT and MPKGRP where ALERT takes higher energy and proposed MPKGRP takes lesser energy than the other.

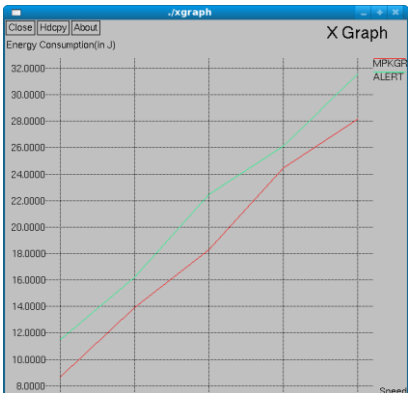

Figure 3: Comparison Graph for Energy

Average Delay

The average delay is calculated by taking the average of delays for every data packet transmitted to the total number of received packets as defined below in equation. The parameter is measured only when the data transmission has been successful.

$$Average\ Delay = \frac{Sum\ of\ All\ Packets\ Delay}{Total\ No\ of\ Received\ Packets}$$

The Figure 4 shows the graph of average delay taken for ALERT and MPKGRP where ALERT takes more average delay and MPKGRP takes less average delay.

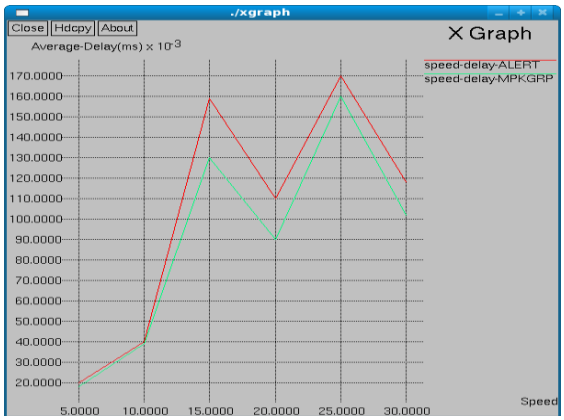

Fig 4: Comparison Graph for Average Delay

Unknown Neighbor Ratio

The Figure 5 shows the graph of unknown neighbor ratio taken for ALERT and MPKGRP where ALERT takes lesser unknown ratio of neighbor and proposed MPKGRP takes higher unknown ratio of neighbors.

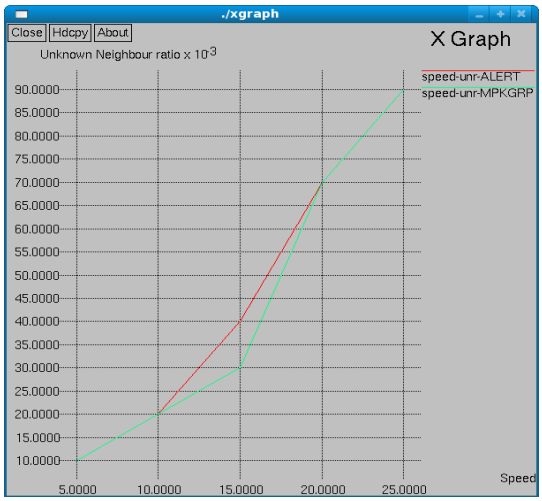

Fig 5: Comparison Graph for Unknown Neighbor Ratio

Packet Delivery Ratio (PDR)

The ratio between the number of packets successfully received at the destinations and the total number of packets sent by the sources defined in equation.

$$PDR = \frac{received\ packets}{sent\ packets} * 100$$

The Figure 6 shows the graph of PDR for ALERT and MPKGRP where ALERT takes low PDR and proposed MPKGRP takes higher PDR.

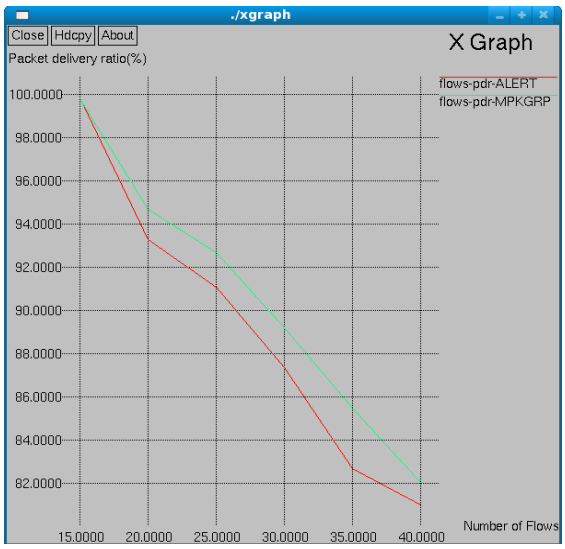

Fig 6: Comparison Graph for PDR

6. Conclusion

The anonymity based MPKGRP routing protocol with mobility prediction model and Blowfish algorithm is implemented in this work to enhance routing performance and security with minimal packet loss and delay. The mobility prediction model is used to predict mobility of node and suppress periodic messaging based on simple linear method. The proposed routing protocol is used to dynamically zone partitions and randomly select relay node for packet transfer. It gives the toughness for an intruder to detect the source and destination. MPKGRP routing protocol provide better security for packet by hiding source, destination node and packet transmission direction. The experimental analysis of MPKGRP is compared with ALERT which shows that proposed MPKGRP minimizes average delay, beacon overhead, energy consumption, and efficient neighbor ratio with higher PDR value.

References

[1]. M. Younis and S. Z. Ozer, "Wireless ad-hoc networks: Technologies and challenges," Wireless Commun. Mobile Computing, 6 (7), 2006, pp. 889–892.

[2]. S. Guo and O. Yang, "Energy-aware multicasting in wireless ad-hoc networks: A survey and discussion," Computer Commun., 30 (9), 2007, pp. 2129–2148.

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

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

[5]. Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.

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

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

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

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

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

[11]. C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., 25 (1), 2007, pp. 192-203.

[12]. X. Wu, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol," IEEE Trans. Mobile Computing, 4 (4), 2005, pp. 335-348.

[13]. B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc. IEEE 29th Ann. Int'l Conf. Local Computer Networks (LCN), 2004.

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

[15]. X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous GeoForwarding in MANETs through Location Cloaking," IEEE Trans. Parallel and Distributed Systems, 19 (10), 2008, pp. 1297-1309.

[16]. S. Ratnasamy, B. Karp, S. Shenker, D. Estrin, R. Govindan, L. Yin, and F. Yu, "Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table," Mobile Network Applications, 8 (4), 2003, pp. 427-442.

[17]. M. Heissenbuttel, T. Braun, M. Walchli, and T. Bernoulli, "Evaluating of the Limitations and Alternatives in Beaconing," Ad Hoc Networks, vol. 5, no. 5, pp. 558-578, 2007.

[18]. B. Blum, T. He, S. Son, and J. Stankovic, "IGF: A State-Free Robust Communication Protocol for Wireless Sensor Networks," technical report, Dept. of Computer Science, Univ. of Virginia, 2003.

[19]. M. Zorzi and R. Rao, "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Energy and Latency Performance," IEEE Trans. Mobile Computing, vol. 2, no. 4, pp. 349-365, Oct.-Dec. 2003.

[20]. M. Heissenbuttel et al., "BLR: Beacon-Less Routing Algorithm for Mobile Ad-Hoc Networks," Computer Comm., vol. 27, pp. 1076- 1086, July 2004.

[21]. P. Casari, M. Nati, C. Petrioli, and M. Zorzi, "Efficient Non Planar Routing around Dead Ends in Sparse Topologies Using Random Forwarding," Proc. IEEE Int'l Conf. Comm. (ICC), pp. 3122-3129, June 2007.
[22]. S. Basagni, M. Nati, C. Petrioli, and R. Petroccia, "ROME: Routing over Mobile Elements in WSNs," Proc. 28th IEEE GlobeCom, pp. 5221-5227, Dec. 2009.
[23]. Haojun Huang, Guangmin Hu and Fucai Yu," Energy-aware geographic routing in wireless sensor networks with anchor nodes", SEP 2011.
[24]. Dengfeng Yang, Xueping, Rapinder Sawhney,Xiaorui Wang, "Geographic and Energy-Aware Routing in Wireless Sensor Networks", International Journal of Ad Hoc and Ubiquitous Computing.
[25]. K.Thamizhmaran, Akshaya devi arivazhagan, M.Anitha," Co-operative analysis of Proactive and Reactive Protocols Using Dijkstra's Algorithm", Recent Advances in Electrical Engineering and Electronic Devices,2014.
[26]. Haiying Shen et al," ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", Mobile Computing, IEEE Transactions, vol 12 (6), 2012, PP.1079 – 1093
[27]. W. Stallings, Cryptography and Network Security: Principles and Practices, 2nd ed., Prentice Hall, 1999