Received: July 9, 2017

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

ArcRectZone: A Lightweight Curved Rectangle Vector Based Secure Routing for Mobile Ad-Hoc Sensor Network

Viji Gripsy Jebaseelan[1*] **Anithalakshmi Srinivasan[1]**

[1]*Department of Computer Science, PSGR Krishnammal College of Arts & Science for Women, Coimbatore, India*
* Corresponding author's Email: gripsyjebs@gmail.com

Abstract: Location aided routing in Mobile-Ad hoc networks are the most significant process because it limits the route search and allows routing with least messages. Due to the dynamic and uncertain infrastructure of Ad-hoc and sensor networks also creates several security issues like route misbehaviors. This paper aims to develop a new lightweight route selection scheme with the security concern. In this scheme, the routing attack targets are identified and avoided by deploying intellectual watchdog and lightweight key verification mechanisms, the scheme also utilizes the curved rectangle zone selection for shrinking route search space. The scheme is extended to adopt the curved rectangle zone routing for both Ad-hoc and Sensor Networks. The core functionality of the proposed work in terms of cost effective and secure route selection is validated by NS-2 tool. The experimental results demonstrated that the proposed approach is cost effective and secure and provides significant performance improvements with least energy consumption.

Keywords: Location aided routing, Security, Mobile ad-hoc and sensor network, Watchdog, Curved rectangle zone, Signature algorithm.

1. Introduction

Mobile Ad-hoc Sensor Networks (MASNet) are infrastructure free and dynamic in nature. The mobile sensing nodes in the MASNET always use a dynamic network topology and perform communication without relay on any static structure [1]. The increasing features and the decreasing costs of sensors make MASNETs applications possible to be deployed in real-world applications. In such scenario, the network reconstruction, security improvements with cost effective mechanism are hard to deploy. Even it is harder when the node has high mobility. Considering every issue in the MASNet may create more difficulty in terms of communication overhead, time consumption, and data management. So, every application under MASNet should contemplate on these basic and essential goals. To attain such goals in both Mobile ad-hoc and sensor networks effective routing protocols are used, this scenario is became called as MASNet. Designing routing protocol for this type of network is more challenging due to several reasons like difference application type, the difference in mobility, range, resource and network size etc. Beyond these issues it also has several security crisis, which are different in wireless sensor and adhoc networks.

In this paper, we propose a routing technique for MASNET that decreases both packet transmission delay and loss due to security issues, with much lesser control overhead than the existing location aided routing mechanism. Our algorithm takes advantage of curved rectangle based routing with the routing security considerations, and with the use of effective signature schemes the location aided routing environment achieves secure data transmission with less overhead. Active and Passive collection of Arcrect zone neighbor node intercommunication will be utilized upon the need to reconstruct any broken link with an immediate neighbor. Hence, we minimize the control packets

needed for local repairs with the cost of some local routing tables.

The rest of the paper is organized as follows. Section 2reviews the existing works on location aided routing. Section 3 gives a description of problem summary. Section 4 describes our proposed algorithm. Sections 5 and 6 contain simulation results and conclusion respectively.

2. Literature survey

There are several research studies developed many protocols for ad-hoc and sensor networks. Many works extends the standard routing protocols of ad-hoc and sensor such as Ad-hoc On demand Distance Vector (AODV), Low Energy Adaptive Clustering Hierarchy (LEACH) and DSDV [2] etc., All the works were aimed at reducing energy consumption at the time of selecting path.

2.1 Extension of leach

In recent past, a number of works have been done on MASNETs along with the evolvement of wireless sensor network [3]. Many works have done particularly in mobile environment networks involving distance or location estimation using various approaches in MASNETs and few used hop count, clustering methods to reduce the network delay. Estimated distance is used to select the nearest next hop node in a mobile environment as the nodes movements are affecting the process of selecting the next hop node for forwarding message from a source to destination. Due to that reason, distance estimation algorithm was taken into places to involve in this research with the presence of current routing algorithm in order to prove that the enhancement has been made to the current algorithm to support energy conservation in mobile ad-hoc sensor networks.

One of the most prominent protocols is the Hybrid Energy-Efficient Distributed (HEED) Clustering, which is a distributed, energy efficient clustering approach. It extends Low Energy Adaptive Clustering Hierarchy (LEACH) protocol [4] by using residual energy as primary parameter and intra-communication cost to cluster the network. HEED consumes a significant part of its energy for the process of clustering [5, 6].

2.2 Hop count based protocols

Authors in the paper [7] briefly reviewed hop count based protocols for MASNET and investigate the performance with the consideration of the hop count shift problem. They mentioned that the problems can obviously be eliminated if all nodes know their Cartesian coordinates via respective GPS units. Here Cartesian coordinates indicate the location of a point relative to the fixed reference point. But, enclosing each node with a GPS is high-priced and it is not reliable. In certain cases, several protocols are designed without the prediction of locations but based on hop count only. Although such kinds of protocols suffer from the inaccuracy of nodes location estimations, the simplicity may still help them with lots of practical usages. Due to that reason, they propose a strategy to battle the hop count shift problem and conduct some simulations to show its effectiveness. Their study suggests that these protocols performance generally suffers from the hop count shift problem.

In [8] authors present the hop count problem in mobile ad hoc network and propose an efficient hop count routing protocol(EHCR) based on the previous studies of mobile ad hoc network. The performance of EHCR evaluated with the existing protocols by using NS2. Their experimental result shows that the program can resolve the hop count problem and improve the network packet delivery ratio, as well as reduce the network delay and overhead. They also improve the overall performance of wireless and network. The issue of energy consumption and the proposed solution of this problem was not mentioned by the authors.

2.3 Distance based protocols

In paper [9] authors used a self-determined geographical forwarding MASNET scheme. In this paper, authors improved the static channel width routeless routing protocol (SCWRR) and proposed a new protocol named as Adaptive Channel Width Routeless Routing Protocol (ACWRR). ACWRR uses a rectangle-shaped broadcasting channel called Route Broadcast Virtual Channel (RBVC). This channel connects a source node to its destination per communication session. Inside RBVC, each hop uses a countdown timer to determine the back-off delay before the node rebroadcasts a (newly received) packet. The countdown timer is a function of the node's remaining energy, location information, and signal strength. This reduces the rebroadcast frequency in a much tighter-controlled geographical flooding to achieve less energy consumption.

In the paper [10], authors obtained the improvement of a newly developed Static Channel Width Routeless Routing (SCWRR) protocol which uses a self-determined Geographical Forwarding MASNET. Even though the previously obtained

results are very competitive with peer protocols, these attempts to explore all venues in order to enhance protocol efficiency, one of such venues is to vary the source-destination channel width. The adaptive channel width simulation results show an enhancement in the power budget of about 10% over the static approach. Such enhancement may prove to be critical in some sensor network applications, making our protocol more amenable in the MASNET domain.

One of the algorithms for location estimation in the area of sensor networks is based on RSSI sampling has proposed in [11]. RSSI model used as the signal was broadcasted by the beacon to all sensors, then distance between sensors and beacon can be estimated on the basis of the signal strength stored along with the process. Furthermore, probabilistic model used to compute a position estimation of the sensor node by sampling multiple readings from beacons. They compute the correct probability distribution of the sensors location and then adopt this probability distribution in a theoretical analysis of sampling the measurements for location estimation. However, they have mentioned in their paper that there are obvious tradeoff occurred between accuracy and power consumption. This happened due to the factor that if higher accuracy is desired, more beacons are deployed or more samples are used. Using a large number of beacons and samples causes significant energy consumption. Other than that, code of the program written in NesC is 47K whereas the amount of memory needed to execute this program in TOSSIM is 637K. One of the works, notably [12] have proposed an enhanced mechanism for a next hop node selection RSSI-based Forwarding (RBF) protocol that works without knowledge of nodes location by using a RSSI level of beacon signals transmitted by the sink. Next-hop node is determined among the forwarding candidates using a timer-based suppression scheme. Improvement of the suppression scheme is proposed as a contender closer to the sink is chosen with higher probability for being selected as a next-hop node. The mechanisms used affect the overall nodes relaying burden, energy consumptions and congestion level in the network.

Finally authors in [13] proposed Rectangular Zone based Location Specific Routing (RZLSR) approach for energy efficient, adaptive and secure route discovery in MASNet. It uses labels to carry the disjointness-threshold between nodes during the route discovery. This process in the approach improves the quality of services over the route discovery. At the time of route discovery, the approach utilizes the RECT scheme for broadcasting. This effectively improves the data routing between the source and destination. Additionally the authors concentrated on a set of security mechanisms. To improve the security the scheme use of Watchdog and digital signature concepts were used. This effectively protects the route discovery process. But the watchdog method created several false alarms and not effective if other security threats arises.

Paper [14] presents a detailed analysis of the Radio Signal Strength (RSS) model for distance estimation in wireless sensor networks through empirical quantification of error metrics. Indeed, on the basis of this experimental analysis, they implement k-nearest signal space neighbor match algorithm for localization, and evaluate some vital control parameters using this technique. This work can be adapted to different cases and scenarios, to achieve finer and more precise location estimates. Their results are encouraging and they are able to achieve an accuracy of nearly 1.1 meters with 90% probability in indoor environment. The theory of distance estimation using RSSI value is almost similar to our project, but we are focusing on the study that energy conservation can be prove by implementing distance estimation algorithm in AODV.

This work [15] authors used RSSI value for distance estimation in Wireless sensor networks based on Zigbee. In regard to distance evaluation as well as routing protocols, RSSI (or LQI) plays a significant role in deciding which link to use next (in multi-hop network) so that packet delivery will be optimal in time or energy matter. The first problem come across in this study was the problem of Microchip documentation and the interpretation of RSSI value. RSSI value is defined in datasheets but never explained as to how to calculate real RSSI value in dBm, in regard to the RSSI given by the MRF24J40 module (which is basically the AD value measured within the module). Some question arises by the researches in this study and they concluded that the distance can be precisely evaluated if the terrain variables and conditions are near perfect. This paper concentrates on evaluating the performance of AODV in MASNETs environment to get a better performance evaluation results on AODV routing protocol. We investigate the impact of running simulation in various time lengths with both hop count and estimated distance routing algorithm, and compare their performance in terms of the average percentage of packet loss and energy consumption. The proposed work is focusing on enhancement of RZLSR with RECT broadcasting

scheme routing protocol to improve energy and packet delivery in mobile communication.

3. Problem definition

In several MASNET applications, energy and security are the major factors. The applications like health data dissemination, environmental data transmission with high mobility factor need more attention on security threats over MASNET. Except few, many kinds of research only concentrated routing efficiency without security considerations. An energy effective routing algorithm is needed to reduce the transmission overhead even with the security process. For cost-effective data transmission, AODV routing protocol is widely used for both Ad-hoc and Sensor Networks. In some papers [16, 17] used multipath routing technique for effective and secure data transmission over MASNET. However, the lightweight secure selection mechanism with all QOS parameter considerations is still challenging. In this paper, we aim to overcome those issues by exploring a new adaptive and reliable routing protocol. This may reduce energy consumption in MASNETs, which helps to reduce the average percentage of packet loss and minimize the average total energy consumption. And specifically, the watchdog technique is not effective to spot false route attack and other misbehaviors. It also raises false alarms in the presence of hazy collisions, conflict with a receiver like spoofing and when the transmission power is limited.

4. Proposed system

Secure and reliable data transmission in MASNET is a challenging task due to its wide variety of attacks and different routing scenarios. In order to provide fast routing and data authentication, a novel routing technique has been introduced. Recently, digital signatures and watchdog methods are observed to provide better results on the security against route misbehaving attacks. These schemes can reduce the route misbehaviors by effectively calculating trust scores. But, the major problem of these schemes in the ad-hoc network is the cost effective secure routing. The proposed developed a new lightweight optimal route selection technique with ArcRect (a curved rectangle zone based secure routing) for MASNET. Many protocols have been designed and implemented to provide secure routing and data transfer, which ultimately results in too much overhead and routing load in the network. Keeping this in view, the **ArcRect** is proposed and implemented to eliminate unwanted computational and processing overheads that degrade the network. The **ArcRect** provides a good packet delivery ratio by choosing highly secure nodes, based on trust to establish an authenticated route, thereby enabling secure data transfer.

4.1 Contributions

- We propose a protocol to improve the routing performance with security considerations according to the drawbacks of RZLSR.
- A new **Intellectual Watchdog Technique (IWT)** is proposed to protect the data from different types of routing misbehaviors with fewer false alarms.
- A lightweight **single bit signature key** verification technique is used to detect route misbehaviors rapidly. Instead of signing every packet it just verifies and updates the last bit. This process can drastically reduce communication and verification overhead.
- Route selection and data transmission performed by ArcRect zone, this will reduce the zone size by producing arc size in the rectangle zone.
- The security and ArcRect zone is integrated with the LAR (location-aided routing protocol).

4.2 Proposed routing process

In RZLSR algorithm, the request zone is defined to be the smallest rectangle that includes the source node and the expected zone, such that the sides of the rectangle are parallel to the X and Y axes. In order to reduce the route searching space, we defined a circled-rectangle shaped request zone. The circled-rectangle shaped request zone is smaller than the request zone defined in RZSLR and LAR and guarantees to cover the source node and the expected zone along with the security considerations. When the route discovery fail in the first attempt, the proposed protocol redo route discovery by flooding that enlarges the request zone to entire network rapidly. We adopted an increment and intelligence search vector mechanism to avoid huge routing traffic and congestion, caused by the flooding policy used by proposed technique. We introduced security scheme to limit the number of malicious participant nodes in the route discovery. And if any failure occurs in the route selection, the RREQ will be performed with two-hop selection. That is it only considers only two-hop not more than that.

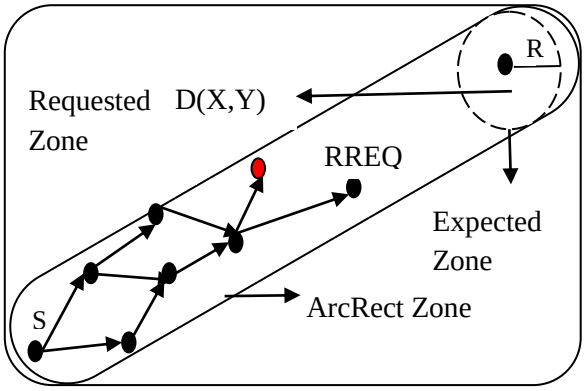

Fig.1 Initial zone detection

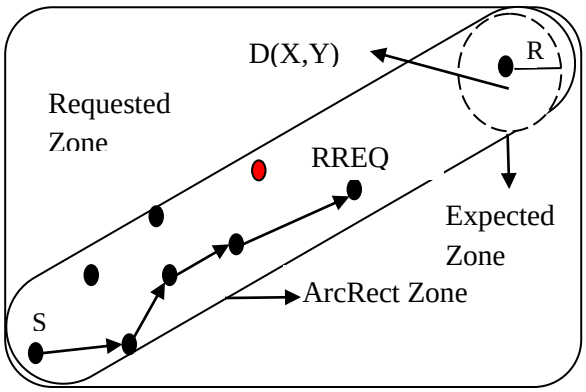

Fig.2 Initial zone detection with security consideration

4.2.1. Phase 1: Network construction and route discovery

The first phase is initial network construction with 50 mobile nodes. The system simulated the proposed scheme by using the ns-2 network simulator. In the simulation, 50 mobile nodes are placed within a square area of 1500 m × *15*00 m. this use Random Mobility model to determine movements of mobile sensor nodes. In the Random mobility model, each node moves to a randomly chosen location with a randomly selected speed between a predefined minimum and maximum speed. After reaching that location, it stays there for a predefined pause time. It then randomly chooses another location after that pause time and moves to that location. This random mobility process is repeated during a simulation time with the above mentioned nodes.

The ArcRect provides a proactive way to protect the data from different attacks. So this initially detects the best path based on the reports of **intellectual** watchdog method. The initial route discovery has the following process.

4.2.2. RREQ

ArcRect routing protocol is based upon distance vector and uses destination numbers to determine the freshness of routes along with the security constraints. ArcRect is capable of both unicast and multicast routing. ArcRect requires hosts to maintain only active routes, for example the route used to forward at least one packet within the past active timeout period. When a host needs to reach to destination and does not have an active route, it broadcasts a route request (RREQ) packet, which is disseminated in the network.

Fig.1 shows the initial zone detection process in ArcRect**.** In this process the source node S broadcasts the RREQ for the neighbor list within the zone. This process also finds the attack free node at the time of routing. Here source node S gets the vector for the expected zone.

4.2.3. RREP

A (RREP) route reply is replied back to the source of RREQ to establish the route in the network. It uses HELLO message along with the security check to determine the connectivity among the neighbors within the request zone.

Based on the RREP, the source node s will optimize the route and transmits the data to the destination R. at the time of data transmission, a single bit key will be verified instead of the whole key size.

The value of evaluating the path in terms of reliable and secure constraints is taken as the initial value in ArcRect, which contains all constraint conditions in searching optimum path. The factor such as path length, number of connections, energy consumption and the node security considerations should be evaluated for feasible path threshold value. The feasible path threshold function of n nodes is defined as follows:

$$f(x) = W_d d(X) + W_e e(X) + W_l l(X) \quad (1)$$

In Eq.(1), w_d、 w_e and w_l are respectively length, ArcRect position and the network security stability. *d(X)* is the path length, *e(X)* is energy consumption of selected path within the ArcRect zone, *l(X)* is the node security stability, the total length of path is as follows:

$$d(X) = \sum_{i=1}^{n-1} d^2(m_i, m_{i+1}) \quad (2)$$

In Eq.(2), $d(m_i, m_{i+1})$ is the distance between the node m_i and m_{i+1}. Network energy consumption is as follows: An initial process selects a path by adopting ArcRect to transmitting data, which is divided into feasible path and unfeasible path by reliable and secure. Packet information for every RREQ process consists of different node sequence, so the length of route is variable and it can be defined in the packet header itself.

4.2.4. Credence verification

In the proposed system, credence verification using single bit key is used. This phase will be used at the time route request. A trust level of network is defined on the bases of previous behavior of the node calculated by the intellectual watchdog mechanism.

4.2.5. Algorithm steps

1. Let N is the wireless nodes in the network
2. Cluster the nodes into k-clusters and set priority p=null
3. Let sender node S broadcasting RREQ to the neighbor list Li
4. For every RREQ in the k-cluster, finds the trust score Ts. And append on the RREP
5. Read hop id, keys and Ts from RREP.
6. Check criteria for security S and Zone size (z).
7. For each node i from node list N do →
8. *If (criteria Sz =RREP(ni))*
    1. *Verify (key(ni))*
        a. Convert the decimal value to a binary value
        b. Break the binary value out into single-bit chunks
        c. Find the last bit value in the key from RREP and verify
        d. Add node into the p=ni
    2. Forward and update if the criteria matches
9. Else
    1. Find next node in N.
10. Update the priority with ts.

This process initially evaluates trust value of each node by a real number *T* with a continuous value between 0 and 1. In this proposal, trust is described by two mechanisms: direct observation trust and indirect observation. These components are similar to those used in existing systems. In direction observation trust, an observer estimates the trust of his one-hop neighbor based on its own belief. So, the trust value is the expectation of a subjective probability that a trusted uses to decide whether a node is reliable and legitimate.

In this illustration, node 1 is an observer node, and node 3 is an observed node. Node 1 sends data messages to node 5 through node 3. When node 3 receives data messages and forwards to node 5, node 3 can overhear it or else node 3 can re transmit the data by performing wormhole and sinkhole attacks. Then, node 1 can calculate the trust value of node 3 based on data messages. The same idea is applied to the control message situation. Meanwhile, IWT collect information from nodes 2 and 4 along with the node 3's previous transactions, which have interactions with node 3 to evaluate the trust value of node 3.

5. Experimental results and analysis

This performed simulations using network simulator. The simulator is written in C++ and implements the code in TCL. The events (nodes meeting, node arrival at its selected destination, and alarms time-out) are pushed to and pulled from an ideal time-line. Initially, nodes are assumed to be randomly deployed over a network area. Then, until the simulation ends, for each node, a random speed and destination location are randomly chosen (within the bounds set by the user): this implies to analyze and to order all the meeting events and the node arrival events with reference to the time-line. While the time goes by, the events on the time-line are processed. The events corresponding to node arrival are processed as previously described (choosing a destination, a node speed, and analyzing the new generated events). Along with 50 nodes has created. The key and route verification events are processed as the main part of the ArcRect, where the lightweight key management and source and destination authentication has been completed.

The ArcRect routing with security process is experimented using network simulator 2 (Ns2). The table 1 shows the list of parameter used for the experiment.

The proposed design is implemented using NS-2 and it is analyzed by considering certain parameters like Packet lost, Packet delivery ratio, Energy consumption and End- to-end delay. In the proposed ArcRect framework selects the best path to reduce the packet misuse problems by several attacks and Packet loss and there by increases the packet delivery ratio with less energy consumption.

The wireless network is created. Mobile nodes are configured with the properties like buffer, antenna etc and randomly deployed in the network area. All the mobile nodes are connected with wireless links.

Table 1. Experiment parameters

Parameter	Value
Simulation tool	NS2
Version	NS 2.35
Antenna	Omni antenna
Channel	Wireless
Number of nodes	50
Communication agent	TCP
MAC type	802-11
LL	Link layer type
Mobile Node location	a) random position, and b) outside network field at the distance of 100 m.
data packet length	It is assumed that each node generates fixed Length data packet of size 1024 bits.

The mobile can act as a data initiator or data forwarder which forwards the data from the other mobile nodes. Create ad hoc networks using random sampling routing protocol with few numbers of nodes that communicate with each other in a wireless environment. It is performed to assess the connectivity of the network. The working procedure of ArcRect is described in the in to two tasks likely as adaptive route and secure node selection.

5.1 Results

The developed location specified secure routing process is experimented and analyzed with different QOS metrics. The route selection processes in MASNET are always needed a high resource and time. But in the proposed system, using the lightweight key verification scheme the time and cost is reduced.

5.1.1. Packet delivery ratio (PDR)

The ratio of number of packets send from source and number of packets reach the destination. The ratio of the number of packets received and the number of packets expected to be received. In the analysis, the PDR ratio is improved in the proposed system when comparing with the existing Rect zone 16] based routing scheme. The impacts of secure routing process, the PDR values are increased.

The packet delivery ratio is calculated as follows:

$$PDR = (No\ of\ packets\ Received / No\ of\ packets\ send) \times 100 \quad (3)$$

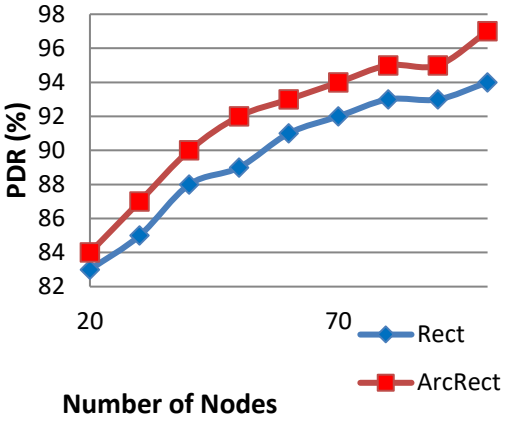

Fig.3 Packet delivery ratio comparison chart

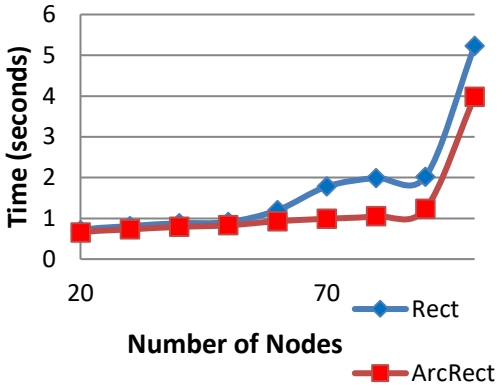

Fig.4 Delay comparison analysis

Fig.3 shows the comparative analysis between the existing Rect zone with watchdog technique and proposed ArcRect with intellectual watchdog technique. The results shows when the node count increases then the PDR ratio will gradually increases. Due to the proactive route selection with reliable and secure node improves PDR ratio than the existing system.

5.1.2. Delay comparison

The proposed system shortens the zone size at the time route selection. The data will be transmitted via the selected secure nodes by the ArcRect Zone. And the data will reach the destination in any of the available best nodes and paths if there are multiple paths available. Thus delay time of proposed system decreases when compared to the existing system. And the authentication process performed by single bit key verification, so the data authentication delay also reduced in the proposed system. Packet transmission delay is calculated as follows:

$$Delay\ (Delivery\ Time) = Receiving\ time - Sending\ time \quad (4)$$

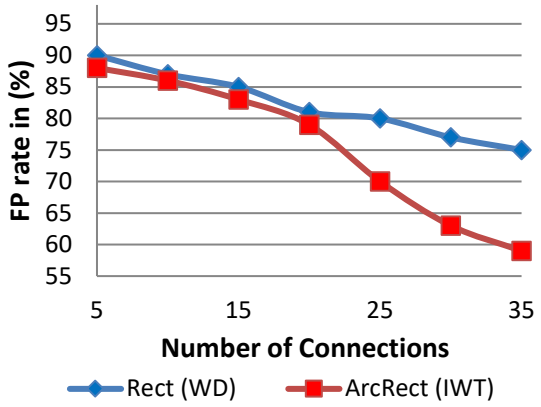

Fig.5 accuracy detection in terms of false positive ratio

Table 2.0 Results from existing and proposed approaches.

Parameters	Techniques	
Total packets	182	195
Received packets	171	190
Dropped packet	11	5
Routing overhead	0.22	0.14

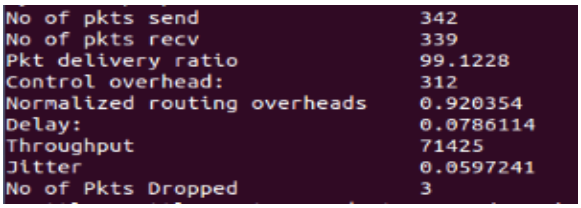

Fig.6 Results of the ArcRect with 50 nodes

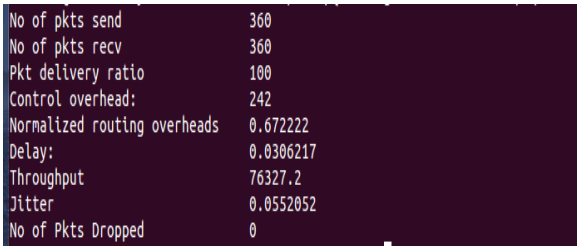

Fig.7 Results of the ArcRect with 100 nodes

Fig.4 shows the delay analysis between the existing Rect zone with watchdog technique and proposed ArcRect with intellectual watchdog technique. With the use of IWT and single bit key verification schemes, the delay is reduced. When the number of nodes increases the delay will also increase. In the proposed work the scalability is achieved due to this fast verification process.

5.1.3. False positive ratio

The main comparison between existing watchdog and proposed intellectual watchdog methods are calculated in terms of false positive ratio. The term false positive ratio is used to find the false alarm ratio at the time of route misbehave node detection, this is the probability of falsely rejecting the node at the time of verification.

The watchdog method always results in higher false alarm. While comparing with the watchdog mechanism, the proposed system improves the detection accuracy. The watchdog mechanism uses only local information and it doesn't aware about the neighbor mobility out of range.

5.1.4. Overall comparison

Table 2 shows the packet received ratio and routing overhead of two existing techniques with the proposed one. From the analysis and comparison, the proposed system yields much positive results in all parameters. The comparative study has done with 50 nodes. From the simulation; the results are gathered for the further analysis with different QOS metrics.

The experiment is carried with 50 and 100 nodes respectively with different resource level. This experiment produces best result in terms of PDR, because if the number of node increased, then the available node count in the ArcRect zone is high, so node availability can increase the data transmission rate. The values are specified in the fig 7.0. The packet delivery ratio is 100% in the second phase of simulation. And 99.123 % when there are 50 nodes. This may be varying according to the total number of nodes and its energy.

6. Conclusion

An improved ArcRect with intellectual watchdog method is proposed in this paper for fast and secure routing in MASNET. An adaptive security aware routing strategy is followed to shrink the routing zone for fast data transmission. The performance of the proposed work is investigated with several QOS factors and proved the proposed work is optimal for MASNET.

The proposed techniques are generated with several QOS considerations such as reducing delay, false alarms with energy minimization. The proposed work achieved highest packet delivery ratio with two different set of nodes connections. The control overhead is adequate and doesn't exceed too much. The result shows the control overhead and false positive rations are reduced when there are many connections between nodes. This clearly shows our proposed work is highly suitable for huge and dynamic networks. This

increases the scalability with effective signature concepts.

In future, the proposed system can be expanded and it has many future directions. The packet delivery ratio in the network determined.

References

[1] M. Carlos and P. Agrawal, "Mobile ad hoc networking", *OBR Research Center for Distributed and Mobile Computing*, pp. 125-186, 2002.

[2] S. Taneja and A. Kush, "A survey of routing protocols in mobile ad hoc networks", *International Journal of Innovation, Management and technology*, Vol.1, No.3, pp.279-285, 2010.

[3] O. Younis and S. Fahmy, "Distributed clustering in ad-hoc sensor networks: A hybrid, energy-efficient approach", In: *Proc. of International Conf. on IEEE Computer and Communications Societies, HongKong*, pp. 879-884, 2004.

[4] F. Xiangning and S. Yulin, "Improvement on LEACH protocol of wireless sensor network", In: *Proc. of International Conf. On IEEE Sensor Communication in Sensor Technologies and Applications, USA*, pp. 260-264, 2007.

[5] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks", *IEEE Transactions on mobile computing*, Vol. 3, No. 4, pp. 366-379, 2004.

[6] R.Tandon, B. Dey, and S. Nandi, "Weight based clustering in wireless sensor networks", In: *Proc. of National Conf. on* IEEE *Communications, Delhi, India*, pp. 15-19, 2013.

[7] R Chaudhary and S Vatta, "Review Paper on Energy-Efficient Protocols in Wireless Sensor Networks", *IOSR Journal of Engineering*, Vol. 4, No. 2, pp. 1-7, 2014.

[8] E.M. Royer and C.K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks", In: *Proc. of International Conf. on IEEE Personal Communications*, pp. 46-55, 1999.

[9] X. Zhang, Z.H. Qian, Y.Q. Guo, and X. Wang, "An efficient hop count routing protocol for wireless ad hoc networks", *International Journal of Automation and Computing*, Vol.11, No.1, pp. 93-99, 2014.

[10] M.A. Otaibi and H. Soliman, "Efficient Controlled Routeless Routing Protocol With Fixed Channel's Width for Mobile Ad Hoc Sensor Networks", In: *Proc. of IEEE ICCCN 09*, pp. 1-7,2009.

[11] C. Papamanthou, F.P. Preparata, and R. Tamassia, "Algorithms for location estimation based on RSSI sampling", *International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics*, pp.72-86, 2008.

[12] A. Awang, X. Lagrange, and D. Ros, "A cross-layer medium access control and routing protocol for wireless sensor networks", *Journées Doctorales en Informatique et Réseaux*, pp. 85-90, 2009.

[13] A.S. Vijendran and J.V. Gripsy, "Rect zone based location-aided routing for mobile ad hoc and sensor networks", *Asian Journal of Scientific Research*, Vol.7, No.4, pp.472-481, 2014.

[14] M. Saxena, P. Gupta, and B.N. Jain "Experimental analysis of RSSI-based location estimation in wireless sensor networks", In: *Proc. of International Conf. On Communication Systems Software and Middleware, Bangalore, India*, pp.503-510, 2008.

[15] K. Benkic, M. Malajner, and P. Planinsic, "Using RSSI value for distance estimation in wireless sensor networks based on ZigBee", In: *Proc. of International Conf. On Systems, signals and image processing, Bratislava, Slovak Republic*, pp. 303-306, 2008.

[16] J.V. Gripsy and A.S. Vijendran, "QUAD Based Secured Multipath Routing Protocol for Mobile Ad hoc Networks", *Information Technology Journal*, Vol.13, No.8, pp. 1-9, 2014.

[17] A.S. Vijendran and J.V. Gripsy, "Enhanced secure multipath routing scheme in mobile adhoc and sensor networks", In: *Proc. of International Conf. on IEEE Current Trends in Engineering and Technology, Coimbatore, India*, pp. 260-265, 2014.