

Ph.D. Research Proposal

Doctoral Program in "Department Name"

Constructing Energy Efficient Clusters with Tunable

Route for Packets Transmission in 3D Mobile Ad Hoc

Networks



<Reg. No of the Candidate>

<Supervisor Name>

<Date of Submission (DD MM 20YY>





I. INTRODUCTION / BACKGROUND

Mobile Adhoc Network (MANET) is a form of wireless communication network that has no static base station or any fixed infrastructure (topology change frequently). However, wireless networks can be used any network topology i.e. infrastructure or infrastructure less Adhoc. MANET does follow ad hoc topology in which collection of mobile nodes support for peer-topeer data transmission and multi-hop communication. The definition of MANET is follows "MANET is a set of independent mobile nodes that are able to make the communication with each other without the need of any centralized server". The basic characteristics of MANET are follows.

- Mobile nodes are deployed separately from central environment i.e. no administration
- MANET has the property of self-configuration either router or host
- Nodes are self-healing through continuous re-configuration
- Incorporate scalability for the development of large-scale network development
- MANET is created on the nature "FLY" on any situation, since mobility is allows multiple mobile devices
- With the use of decentralized network environment, computation and communication cost is very less

In the context of MANETs, numerous security issues have been widely surveyed. One of the most momentous issues is the presence of malevolent mobile users to disrupt the communications. Most of the security approaches have been widely concentrated to remove all misbehaving nodes in network. In data transmission, each node need to monitors the behavior of adjacent nodes constantly and passes information about suspicious activities to all nearby nodes.







Fig 1 Mobile Users Environment in Energy Sources

There are more than a few reasons to develop a secure MANET model for mobile users because unauthorized devices participated in network for the aim of launching attacks (e.g. spoofing attacks). In view of security requirements, now it is clear that security is a mandatory constraint in MANET and security model avoids the attacker's involvement. In addition to security, other challenges involving in MANET are follows.

- Quality of Service (QoS)
 - High packet delivery ratio
 - Low packet loss ratio
 - Low energy consumption
 - Low latency

1.1 Research Outline & Scope

Make active honesty of mobile user is an inspiring issue since mobile users are dynamic in nature. A designed MANET must ensure reliability, security and privacy for providing services and applications.

1.2 Research Objectives

- To accomplish high QoS, energy-efficient clustering and secure routing mechanism is offered over 3D MANET
- To decrease energy consumption at every nodes, clustering is develop utilizing multiobjective
- To increase the PDR, least amount hop-count based optimum route is implemented from source to the destination nodes.



• To decrease any malfunctions (packet loss, and latency) in MANET, trust management (node authentication and data confidentiality) and message authentication (Data Integrity) is engaged in network. Lately, false data packets are injected at intermediate nodes in transmission, which increases packet loss rate, routing overhead and end-to-end delay. En-route filtering is a new direction in MANET, which is focused on this thesis owing to more progress QoS. Message authentication and trust management is accomplished in MANET by a lot of ways i.e. steganography (digital watermarking) and cryptography mechanisms (digital signature generation and packets encryption)

1.3 Applications / Use cases

At this moment, MANET has huge amount of potential to work on many applications. In below, there are very few applications are given as a reference,

- Healthcare Applications Distributing information among vehicles fin real-time
- **Military Applications** MANET allow for battle communications (military) in order to maintain information. For instance, planes, tanks and soldiers
- Education Applications Conferences and Virtual Classrooms
- **Industrial Applications** Nowadays, MANET is used for commercial application developments. For instance, disaster relief applications.

II. RESEARCH GAPS

2.1 Common Problem Statement

A set of QoS requirements are need to meet by the network while transferring a packet stream from a source to a destination node. For MANET users, it needs for several kinds of services to the users.

2.2 **Problem Definition**

In [1], a multi-criterion with fuzzy based energy efficient routing protocol is proposed for routing in ad hoc networks. In routing, path selected based on the following constraints: hop



count, bandwidth, buffer occupancy, and battery life. In route discovery stage, fuzzy logic based protocol is applied for optimal route selection whereas in route maintenance stage broken links handled and it improves the network performance.

Problems

Delay is high for a single data transmission due to the usage of large number of rules (3⁴)
= 81 rules (Overall system time slows down when the number of rules increase)

Proposed Solutions

• SARSA algorithm is proposed for routing in which we consider the following parameters for selecting the path: Hops count, Delay, Trust Values, Residual Energy. The main advantage of using this algorithm is to uncertainty since it handles uncertainty problem using action value function.

In [2], an enhanced ant colony optimization algorithm is presented to reduce the communication overhead among multiple nodes. This is done by cluster formation and predicting mobility of node. A dynamic mechanism is designed using one or more heuristic parameters for improving the performance of MANET. Then the dynamic list of nodes is maintained during cluster formation (cluster head selection and forming cluster members). Additionally, a hybrid ant colony algorithm is incorporated to provide the status information about the nodes. The concept of Fuzzy with ACO attains correct delivery of packets without any delay.

Problems

• In dynamic cluster formation, nodes in a cluster could move on to other regions. In such situations, CH election process has to be started all over again so here overall delay is high.

Proposed Solutions

• CH election process is simple and efficient using Black Widow Optimization algorithm



Authors proposed a fuzzy logic based reliable routing protocol (FRRP) [3] for mobile ad hoc networks in which stable routes selected. The proposed algorithm is based on the cooperation of autonomous nodes. The score value is evaluated using four criterions: the amount of energy of battery, dynamicity of nodes degrees, accessible bandwidth, and nodes speed. The proposed protocol was to the reduce routing overhead.

Problems

Routing efficiency is extremely low due to the following reasons:

- Incomplete knowledge of nodes
- Less efficiency in membership functions so that here tuning of membership functions are highly required
- Fuzzy rules should be updated with time

A cuckoo search based routing is proposed in [4] MANET. Cuckoo search algorithm reduces time consumption and guaranteed for efficient routing. In this paper, authors presented two phases. In the first phase, cuckoo search based routing is implemented and the second phase evaluate its performance. AODVCS algorithm is outperforms than the previous approaches such as DSDV, and AntHocNET in terms of delay.

Problems

• Not met the energy efficiency problem and also CS algorithm provides slow convergence rate

Proposed Solutions

• We satisfy all the Quality of Service metrics: Delay, Energy Efficiency, Packet Delivery Ratio and Throughput.

In this paper [5], authors proposed identity based cryptography system for consistently deals out the ability of multiple nodes in a network. The proposed mechanism is threshold based cryptography where any identity may help as a public key which increases node security level. It



removes the need for public key certificates and certification authority. User's public key and private key is depends upon their individuality.

Problems

• Identity based Cryptography scheme is less efficient and time consuming

Proposed Solutions

• We proposed two kinds of security: Trust Management by calculating node's trust value and also applied Data encryption using Two Fish Scheme.

Authors considered refinement parameter [6] for trust based routing. Bayesian probability is introduced for trust management and also it provides a reliable network to transmit packets. In this algorithm, packets route from the source to destination through the reliable route not by shortest route. Moreover, uncertainty is handled by computing the trust value and packets are not forwarded through the shortest path.

Problems

- Obtain probability value using Bayesian probability function which leads to more complex and time consuming
- Trust value is calculated using history of nodes behaviour. However, trust management schemes require continuous updation.

Proposed Solutions

- We consider Trusted Authority to monitor the node's trust level. In Time_Interval basis, we update the node's trusted value. At every stage, distrusted nodes are removed from the cluster (if it less the Trusted_{Threshold})
- The proposed research work is novel which is no complex and applicable for large scale networks

III. RESEARCH CONTRIBUTIONS



To overcome the problems in problem definition section, the proposed work is designed with novel and hybrid algorithms. The proposed Mobile Ad Hoc Network (MANET) completely focuses on minimization of energy consumption of nodes. Thus, it considers **3D MANETs** where mobile nodes distributed and move within 3D space. The packet delivery delay and energy performance have been extensively improved in this 3D MANETs. In this design the dynamic mobile nodes are deployed over the 3D network. Initially we start with the cell clustering.

Each cell elects a Cluster Head (CH) based on the following metrics: Node distance, Node mobility, Node Residual Energy. Firstly, we compute those values separately and then compute the Black Widow Optimization Algorithm. The higher fitness value is elected as a Cluster Head. Here we consider two cases. The first case is "if the energy level of current CH is drained, then the next CH is elected based on the Node Residual Energy level". The second case is "if two CHs are within the same coverage, the current Delay Timer is used". Then we introduce a new routing algorithm named Selective Relay Selection by Tunable Parameters by multiple objectives: Node Delay, Node Distance, Node Stability, Node Mobility, and Node Degree. Here, Deng entropy is adaptively tune parameters of node stability and mobility. For complete route selection, SARSA algorithm is proposed. Here we apply Routing Policy based on State and Action values. Most of the existing routing protocols for mobile ad hoc networks have focused on finding the shortest route from a source to destination. The proposed routing scheme has determined the best route with shortest, reliable and stable route. In the proposed research work, nodes behaviour analyses and monitor continuously. Believe value is calculated using history of the nodes. Before transmission data packets are encrypted using Two Fish Encryption Algorithm. Data packets encrypted by three input parameters: Data_length, Data_occrence frequency, and Data Capturing Time.

Performance Evaluation

Finally, our proposed work effectively perform clustering and routing with satisfy the energy efficiency, security and reliability challenges and hence it reduces the energy



consumption and delay and improve the packet delivery ratio in the 3D MANETs. The following metrics are considered in this work,

- Energy consumption
 - With respect to number of nodes
 - With respect to simulation time
 - With respect to attackers rate
- Throughput
 - With respect to number of nodes
 - With respect to simulation time
 - With respect to attackers rate
- End to End Delay
 - With respect to number of nodes
 - With respect to simulation time
 - With respect to attackers rate
- Security Strength
 - With respect to Key length
 - With respect to Bits Size EARCH PARTN

SYSTEM ARCHITECTURE



🔀 phdprimehelp@gmail.com

+91-97 91 62 64 69



IV. RESEARCH NOVELTIES

- In this work, 3D MANET is built with determining the best and the shortest path from source to the destination in MANET is presented in this research. A good path typically has low energy consumption, delay, congestion traffic and high throughput and packet delivery ratio. This is achieved by tunable route selection parameters such as node residual energy, distance and mobility.
- Further, constructing clusters using optimization algorithm which uses multiple objectives such as node mobility, and residual energy.

V. PREVIOUS WORKS & LIMITATIONS

Paper 1

Title: Energy efficient clustering and secure routing using reinforcement learning for threedimensional mobile ad hoc networks

Concept

In this paper, authors propose an energy efficient cluster based secure routing by means of reinforcement learning in 3D MANET. At first, 3D cells clustering is implemented by using





node residual energy, distance and mobility. For this, firefly with cyclic randomization is proposed. A novel routing is proposed which is executed using deep reinforcement learning. Data packets are encrypted by watermarking scheme, which invokes by three processes such as watermark generation, embedding and extraction.

Limitations

• Watermark scheme consumes more energy and delay

Paper 2

Title: Energy Efficient Secured Routing Protocol for MANETs

Concept

In this paper, authors proposed energy efficient secure optimized link state protocol for routing. The objective of this protocol is to provide secure path which is energy efficient and without relying on the third party. In this approach, each node chooses MPR (Multi-Point Relay) nodes amongst the set of 1-hop neighbors. Group key distribution process is invoked to reduce energy consumption and periodically avoids non-authorized nodes. Then they used secure source anonymous message authentication scheme for both message sender and message recipient.

Limitations

• The concept of MPR scheme is worthy because it increases computing ability but bandwidth of network is still insufficient for secure routing

Paper 3

Title: Fuzzy based detection of malicious activity for security assessment of MANET

Concept

Authors had presented a new type of clustering which is called Hierarchical Clustering Routing Protocol. It is supported at large scale MANETs and it is comprised cluster head, cluster gateway nodes, cluster guest nodes, and cluster members. This Hierarchical Cluster based Routing



Protocol follows proactive routing Algorithm among nodes (individual clusters) and reactive routing Algorithm among clusters. Experimentation results shown in the Hierarchical Clustering Routing Protocol provides better performance owing to the combination of two routing Algorithms.

Paper 4

Title: Public String based Threshold Cryptography (PSTC) for Mobile Ad hoc Networks (MANET)

Concept

Chauhan et al. (2018) has worked on their research for secure communication. This follows public key Algorithm with threshold approach to ensure robustness, security and message privacy. This public key cryptography is simulated in NS2 simulator and differentiates attacker nodes from the normal nodes using trust values.

Limitations

• However, public key based cryptography mechanism does not provide high security in packets transmission. UP RESEARCH PARTNER

Paper 5

Title: A secure and efficient cluster based location aware routing protocol in MANET

Concept

Authors had modified the existing algorithm called "Location- based Routing", which is newly introduced as "Secure Location Aware Routing Protocol". This protocol initially initiates the process of clustering. For that process network is partitioned into number of clusters. Node mobility is controlled and managed by PSO in which node future location is predicted. For optimum route selection, link lifetime, node speed, position, and distance to the nearest nodes are computed. Furthermore, trust value is calculated which is useful in future location prediction. When malicious nodes are identified in network, it's removed or isolated from cluster. Data



packets encryption is performed using ECC. Finally simulation is conducted to prove the performance of the proposed approach in terms of energy consumption, packet delivery ratio, delay, and so on.

Paper 6

Title: Multipath security aware routing protocol for MANET based on trust enhanced cluster mechanism for lossless multimedia data transfer

Concept

Authors have proposed a multipath secure routing, which is accomplished by Trust Enhanced Cluster Management (TECM). This model was implemented in a real-time application called Lossless Multimedia Data Transfer Application. Before multipath secure routing, clusters are formed using PSO algorithm. The major drawback of PSO is that it takes large computational time for packets transmission and also it is not effective to transfer packets with minimum energy consumption.

Paper 7

Title: A New Energy based Power Aware Routing Method for MANETS

Concept

Dynamic energy consumption with AODV and PSO algorithms were used (Deep et al. 2018). The main goal of these routing algorithms was to select the optimum path between the source and the destination node. When the network size is increased in MANET achieving QoS is a challenging, since communication overhead among nodes is high and also it leads to high energy consumption.

Paper 8

Title: RAD: Reinforcement Authentication DYMO Protocol for MANET

Concept





Authors presented a new authentication protocol (DYMO) for MANET by reinforcement learning. This Dymo protocol is based on the on-demand routing protocol and dynamic hashing method. Without third party server, encryption technique is proposed to generate and distribute a secret key. By reinforcement learning, node reward is computed. In simulation, it is proved that it shows remarkable achievement in path security in average throughput and packet delivery ratio.

Paper 9

Title: A Secure Identity-based Deniable Authentication Protocol for MANETs.

Concept

Authors investigated a secure identity based deniable authentication (IBDA) protocol to protect the network from malicious activities. The IBDA protocol support for high efficiency and security and it follows the elliptic curve cryptography procedure and identity based cryptosystem (IBC). The IBDA protocol solves Elliptic Curve Discrete Logarithm (ECDL) and Diffie Hellman problem. Due to the security, it is supported for many real-time applications.

Paper 10 YOUR RESEARCH PARTNER

Title: A Novel Authentication and Security Protocol for Wireless Adhoc Networks

Concept

Amin et al. (2018) presented a secure authentication scheme for data transmission in MANET. In this scheme, two operations are designed including authentication and communication. In authentication, mobile nodes are authenticated through their credentials and communication is made by using symmetric cryptography algorithm, which encrypts data packets before transmission. In this way, data confidentiality is preserved. For every communication to the nearby nodes, third party server verifies the authentication for it.

Paper 11



Title: FAPRP: A Machine Learning Approach to Flooding Attacks Prevention Routing Protocol in Mobile Ad Hoc Networks

Concept

Luong et al. (2019) have studied about the routing attacks prevention in MANET. Flooding attacks are one of type of routing attack, which behavior is to broadcast attack packets from one to another. This paper has used an improved version of AODV routing protocol that created for flooding attack mitigation. Experiments are conducted and verified using network simulator that reaches up to 99% of detection rate. In general, flooding is a starting stage of an attack that can be prevented by packet header details.

Limitations

• Flooding attack prevention is detected by simply, but it does not find any new kinds of attacks because packet header can be easily modifiable.

Paper 12

Title: QoSTRP: A Trusted Clustering based Routing Protocol for Mobile Ad Hoc Networks

Concept

Raja et al. (2018) have presented a trust-based clustering protocol for packet transmission and attack detection in MANET. A novel trust management is invoked in which trust values are computed. When the node hashes high trust degree, then it's considered to be normal nodes. Otherwise, it announced as the non-trusted nodes throughout the network. Experiments have conducted to obtain the best performance in terms of packet delivery ratio, energy consumption, throughput, and delay.

Limitations

• The mobile nodes behaviors and their activities are not a constant, which causes forged opinion to someone.



Paper 13

Title: Detection and Prevention of Man-in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in Artificial Neural Networks (ANN)

Concept

Sowah et al. (2019) studied about the intrusion detection and prevention in MANET using ANN especially mitigates man-in-the middle attacks (MIMA) and balck hole attack. In ANN, Intrusion Detection, Identification, Blacklisting and Node Configuration are explored for a dataset with different network traffic. In experiments, it is shown the attack detection rate is 88.35%. Simply, there are three steps are used such as Attack Simulation, Attack Detection and Attack Recovery.

Paper 14

Title: An efficient mobility aware stable and secure clustering protocol for mobile ADHOC networks

Concept

OUR RESEARCH PARTNER

The proposed EESSC technique is proposed which uses fuzzy scheme for selecting cluster heads and it is selected for five kinds of variables such as node remaining energy, node degree, distance, node mobility and trust level. A standby CH is act as again chosen for data collection and transmission. The experiments conducted for diverse of aspects and compared to similar clustering approaches

Limitations

• Energy consumption rate for stable CH is very high

BIBLIOGRAPHY

Geetha N, and Sankar A, "A Multi Criterion Fuzzy based Energy Efficient Routing Protocol for Ad Hoc Networks", Intelligent Automation and Soft Computing, 2017



- Sathiamoorthy, B. Ramakrishnan, "Energy and Delay Efficient Dynamic Cluster Formation using Hybrid AGA with FACO in EAACK MANETs", Volume 23, Issue 2, PP. 371-385, 2017
- Solmaz Ghasemnezhad, Ali Ghaffari, "Fuzzy Logic based Reliable and Real-Time Routing Protocol for Mobile Ad Hoc Networks", Wireless Personal Communications, PP. 1-19, 2017
- Akram Kout, Said Labed, Salim Chikhi, El Bay Bourennace, "AODVCS, a new bio-inspired routing protocol based on cuckoo search algorithm for mobile ad hoc networks", Wireless Networks, PP 1-11, 2017
- Lakshman Narayana, C. R. Bharath, "Identity based Cryptography for Mobile Ad Hoc Networks", Journal of Theoretical and Applied Information technology, Volume 95, Issue 5, 2017
- Priya Sethuraman, N. Kannan, "Refined Trust Energy Ad Hoc on Demand Distance Vector (ReTE-AODV) routing algorithm for secured routing in MANET", Volume 23, Issue 7, PP. 2227-2237, Wireless Networks, 2017
- Muneeswari, B., & Manikandan, M. S. K. (2019). Energy efficient clustering and secure routing using reinforcement learning for three-dimensional mobile ad hoc networks. IET Communications, 13(12), 1828–1839
- Tejpreet Singh, Jaswinder Singh, Sandeep Sharma, "Energy Efficient Secured Routing Protocol for MANETs", Wireless Networks, Springer, Volume 23, Issue 4, PP. 1001-1009, May 2017
- Dhananjay Bisen & Sanjeev Sharma, 'Fuzzy based detection of malicious activity for security assessment of MANET', National Academic Science Letters, pp. 1-6, 2018
- Chauhan, GK & Patel, SM 2018, 'Public String based Threshold Cryptography (PSTC) for Mobile Ad hoc Networks (MANET)', Second International Conference on Intelligent Computing and Control Systems (ICICCS).



- Jamaesha, SS & Bhavani, S 2018, 'A secure and efficient cluster based location aware routing protocol in MANET', Cluster Computing, pp. 1-12.
- Vallala Sowmya Devi & Nagarathna P Hegde 2018, 'Multipath security aware routing protocol for MANET based on trust enhanced cluster mechanism for lossless multimedia data transfer", Wireless Personnel Communications, vol. 100, no. 3, pp. 923-940
- Deep, J & Sutha, J 2018, 'A New Energy based Power Aware Routing Method for MANETs', Cluster Computing, pp. 1-8
- Hamamreh, R. A. Ayyad M. and Jamoos, M. (2019). RAD: Reinforcement Authentication DYMO Protocol for MANET. International Conference on Promising Electronic Technologies (ICPET), Gaza City, Palestine, 136-141.
- Gupta, D. S., Islam, S. H., & Obaidat, M. S. (2019). A Secure Identity-based Deniable Authentication Protocol for MANETs. 2019 International Conference on Computer, Information and Telecommunication Systems (CITS)
- Amin, U., & Shah, M. A. (2018). A Novel Authentication and Security Protocol for Wireless Adhoc Networks. 2018 24th International Conference on Automation and Computing (ICAC).
- Luong, N. T. Vo, T. T. & Hoang, D. (2019). FAPRP: A Machine Learning Approach to Flooding Attacks Prevention Routing Protocol in Mobile Ad Hoc Networks. Wireless Communications and Mobile Computing, 2019, 1–17.
- Raja, R, Ganesh Kumar, P, (2018). QoSTRP: A Trusted Clustering based Routing Protocol for Mobile Ad Hoc Networks, Programming and Computer Software, 44(6), 407-416
- Sowah, R. A., Ofori-Amanfo, K. B., Mills, G. A., & Koumadi, K. M. (2019). Detection and Prevention of Man-in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in Artificial Neural Networks (ANN). Journal of Computer Networks and Communications, 2019, 1–14.
- S, Nagendranath & Babu, A.. (2020). An efficient mobility aware stable and secure clustering protocol for mobile ADHOC networks. Peer-to-Peer Networking and Applications. 1-8.