Optimized Fuzzy based Malicious Node Detection on Routing and Certificate Authority based Secure Communication in Wireless Ad-HOC Network

K. Rajkumar, M. K. Jeyakumar

Abstract— ***The general behavior of Mobile AdHoc Networks (MANETs) is different in certain stages due to its mode of operations and maintenance as well as factors such as Node-Energy level, manipulation energy, randomly movable nature and the topology-changes. These type of dynamicity causes or needs over concentration and needs more security with routing-stability. For eliminating these issues and improve the security, a new methodology called Fuzzy Secured Node Selection Routing (FSNSR) is defined, which provides the Trusted-Network-Service and better performance with energy efficiency in security and dynamicity perspectives. This algorithm FSNSR provides high-reliability and dynamicity to nodes, which can move frequently without any security causes and attain more robustness during performance. The selection of next node selection and forwarding is purely based on the link-stability and next-neighbor availability, which is ensured by means of the parental node by sending route-request and getting response for the request. Once the neighbor provides the response properly for the raised request the node will be treated as a next successful neighbor, otherwise the node will be considered as a malicious node and which cannot be considered for next process further. The survey results further to guarantee regarding the network robustness, dynamicity, good packet delivery ratio, goodput and secure-routing over MANET with the help of Fuzzy Secured Node Selection Routing.***

Keywords— ***Energy Efficiency, Fuzzy Secured Node Selection Routing, FSNSR, Goodput, Mobile AdHoc Network, MANET, Malicious, Secure Routing.***

I. INTRODUCTION

In this modern-world, gadgets like laptops, cell-phones, tablets are playing the major roles in everyone's life, it leads a necessity of "Mobile-Ad-Hoc-Networks" and it provides a wide-variety of support to vehicular-networks as well. This kind of approaches is helpful in many real-time and survival-applications such as disaster-management, squad areas, defense fields and many more. In this supportivity and necessity needs a powerful network-platform called MANET, which provides mobility, connectivity and robustness to all application devices around the world. The term "Mobility" needs to take care about certain causes, which provides crucial effects over network such as Battery-Draining, Mobility-Range, Communication-Efficiency, Energy Sufficiency and so on. Through radio-frequency signals only the MANET is operating and the node-communications are established via radio-signals alone [1]. Usually the MANET based node communications follows MultiHop communication scenario, which forwards data/packets to multiple ways and all will reach the destination more safely without any security issues. The node-formation of MANET is entirely different from other network scenarios, which forms the node in disjoint-way and all the nodes in MANET are self programmed and dynamic in nature, which requires only low-level of radio-frequency levels to make data-transactions with each-other more efficiently. Hence all the network process such as topology-identification and manipulation, route-establishments, message-delivery and all carried out by each node by their own. Thus the MANET is always considered to be robust and self-programmed network. This kind of network needs more concentration over security and energy level maintenance due to its dynamicity, mobility nature and complexity rises mainly in energy management to provide sufficient power for data-transmission between nodes in the network.

The traditional wireless-adhoc network designs are considered mainly on user-friendly nature and attaining more coverage ranges to provide better support to their consumers, but the lacking raises in security and robustness. Those stages of network design is considered as a crucial stages, because the attack possibilities are high and reliability is low in nature and the-network cannot guarantee for vulnerability issues such as malicious interventions, node-mobility, route-manipulations with flexibility maintenance and so on [2][3]. In the present network scenario faces several complications due to its security lacking, many researchers are still developing several techniques to prevent the attacks and safeguard the network from attacks such as intrusions and malicious activities by means of enabling the firewall-operations, Authentication-and-Authorization principles, Access-Control Strategies, Encryption-and-Decryption logics, Trust-Manipulation process and so on.

This all strategies are defined based on the consideration of avoiding malicious activities and provide good support to network consumers and their communication needs. However, the network-protocols present in the current scenario is not sufficient to enable the security norms over

Revised Manuscript Received on August 05, 2019.

K. Rajkumar, Research Scholar, Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil-629180, Tamilnadu, India.

Dr. M. K. Jeyakumar, Professor, Department of Computer Applications, Noorul Islam Centre for Higher Education, Kumaracoil-629180, Tamilnadu, India.

Mobile-Ad-Hoc-Network due to its inefficiency, delay and security lacking, which cannot be provide safeguard to present network scenario to avoid intruders and attackers. Hence there is a necessity to develop a new protocol standard to provide efficient support to MANET to establish the communication in trust-worthy manner and provides best support to its consumers to work with malicious-free and intruder-free network environment and the-proposed mechanism needs to be concentrated on energy-efficiency over mobility and battery-life maintenance. Several researchers quoted or highlighted in their research works like Turst-Establishment and Trust-Manipulation are the most importance concerns we need to take care over MANET and its routing-procedures [4]. The usual network scenario consider the route-establishment process by means of the following way such as network formation, parent node (sender) start communication with next neighbor and it continuous until the destination (receiver) port reached, in this case in between any neighbor creates an issue means the parental node forward the further packets to next possible route to reach the destination and usually the measuring level of trust is always considered to be 0 and 1. If the measuring ratio results in 1 means it is trustable or else the measuring ratio will result in 0 means it is non-trustable. The concept of Fuzzy is quite different from other well-known algorithm logics, which consider the problem in both ways like half-positive and half-negative. So that in both ways it manipulate the results and provides best solution to its approachers. The mentioned node with the trust ratio of 1 is always treated as a Fuzzy-Trusted-Node (FTN) otherwise the node which holds the trust ratio of 0 is always considered as a Fuzzy-Untrusted-Node (FUN) [5]. In past research scenarios, many analyzers analyze the process of network-manipulation using trust-establishment services intended to find-out the trusted-genuine-users and malicious-users. In addition, intrusion discovery frameworks are helpful to recognize the untrusted-nodes which become pernicious and they decrease the network-performance through malicious-activities. In the past, intrusion-identification frameworks have been sent either at the server or at the host-side. Such frameworks were intended to catch the pernicious exercises completed by both inside-clients and outside-clients. In trust-management frameworks, insider-attack possibilities are observed more for performing trust-based-secure-routing.

Energy-Management is the most important need of Mobile AdHoc Networks, which plays a vital role in network improvements, security and node lifetime enhancements. Even the past research of MANET also sustain more concentration on energy-efficiency and route-management with energy aspects to avoid DoS-attacks and flooding-attacks over the network environment. Usually the energy lacking is caused via DoS attacks, which reduces the node energy and trying to make attack the network via that affected node. The node which affects from the Dos type of attack is considered usually as a weak-node and all the attackers trying to affect that node alone to enter into the network and produce further damages over the mobile network and reduce its robustness/stability. The network stability is usually estimated by means of its performance and the overall node activeness in the scenario, even one node failure is also treated as a network affection/failure, which causes the defect in total network scenario and its operations. Mainly, intrusion is the crucial cause of network, which focuses on the weak-nodes in the network and tries to affect the node first and then proceed to further by means of spreading its harmness and finally resulting the network damage or other crucial harmness. So, that an intelligent Intrusion-Avoidance-Scheme (IAS) scheme is also need to be proposed to avoid this kinds of attack over MANET and provide safeguard to the data communication over that network. The proposed scheme should be take care about energy-efficiency, route-management, trustworthiness and mainly concentrate on intrusions, which provides an secure model to Mobile AdHoc Network to enhance their security mechanisms and enhancement of network-performance.

This survey guarantees the Energy-Efficient network-performance with security-enhancements by means of its proposed analysis called Fuzzy Secured Node Selection Routing (FSNSR), which solves the security issues and provides trustworthy routing-service to the network users by means of the following way. The fuzzy schema is always a neutral schema, in which it acts as a questioner and answerer. In network transmission it consider all nodes are untrusted, so that for every communication it acts like first sending empty-packets to make the route-request to the next possible neighbor node and awaiting its response, once the responder node response for the raised request it will be treated as a Successful-Trusted-Neighbor otherwise if any mismatching cases happens, it will be treated as a Untrusted-Failure-Node. By this way, Fuzzy examines all the network transmission clearly and efficiently with the help of AdHoc On-Demand-Distance-Vector (AODV) network-routing protocol [6], which allows the fuzzy to operate based on the network demands and provides successful solution to the network issues such as security, energy-problems, routing-issues and so on. The AODV routing algorithm clearly mark all the network activities in proper trace files, which is helpful to the network configurations to identify the nearest supportive neighbors, position of neighbors and distance between parental node and neighbors etc. The proposed approach assures reliable-routing, data-security by means of cryptographic principles with secured communication process and wireless-network-node mobility-monitoring.

The rest of this survey has been portrayed in the following way such as Section 2 summarizes the Literature Survey, which covers the areas like intrusion-identification-and-prevention, trust-worthy network behavior-management', 'Secure and reliable' routing and etc. Section 3 clearly explains regarding the existing-system and proposed-system, which cover the flaws in existing work and how to solve those network flaws using FSNSR algorithm. Section 4 describes-clearly regarding-the conclusions'-with-future-scope of the proposed work.

II. LITERATURE SURVEY

Power-consumption based-simulation replica for mobile-ad-hoc-network - Kumar K, Singh V - 2014 [11]. Power-problems are considered to be the major threat of network environments. This paper fully concentrates on Power problem over the mobile-ad-hoc-networks, which is considered as a crucial problem over here and it causes severe affection over battery levels, so the node failure can easily happen over these circumstances [11]. There are many topological-prevention algorithms are considered to-prevent these issues and also the main concentration falls on Grid-based-Energy-Aware-Node-Disjoint-Multipath-Routing methodology is applied over here to eliminate the process of node failures due to power problems. In this paper [11], a new congestion elimination model is proposed with scheduling process, so that the issues raised due to power is highly eliminated. The major benefit mentioned in this paper-is: network-lifetime-improvement, reduce the transmision-time and power-optimization. The disadvantage consideration for this work is poor performance during implementation level and causes slow in working like the simulation nature.

A job-market-signaling'-scheme for incentive as-well-as-trust-management in VANET - Haddadou.N', Rachedi.A', Ghamri-Doudane Y - 2015 [12]. In this paper, an asymetric model of Distributed-Trust-Model ('DTM') [12] is taken into account, which is gathered from the classical job-market-signal-replication. This process mainly focused on two things such as Cost expensiveness and node-cooperation based on selfish-node handling model. And also this system monitors the principles for malicious node management in this work and signal processing nature. The main algorithm applied here-is Diffusion-Data-Algorithm and the main advantage of this approach-is: the proposed system eliminates the-cost-expensiveness as-well-as find-out the-misbehavior-node effectively and the disadvantage found in the work is limited range of data transmission and low data rate over network environments [12].

“FBeeAdHoc”: ‘Secure’ Routing-Definitions for "BeeAd-Hoc" based’ fuzzy logic’ in MANET’s - Rafsanjani.M. K', Fatemidokht. H' - 2015 [13]. This paper mainly concentrates on security-threats and vulnerabilities of "BeeAdHocis", which is more crucial in the sense of its identity lacking. This malicious mean hide its identity and the network looks-similar to-normal protocol operations over transmission. The main algorithm/technique applied into this paper is called "FBeeAdHoc", which is implemented using MATLAB and proves that the-present-implementation-is better than the classical routing algorithms. The major benefit noticed in this-paper is talking about Selfish node identity tracking and malicious node identity tracking as well as optimization. The major disadvantage found in this work is improvements required over Selfish node finding principles and time-efficiency during network-transmissions. This paper also discusses, further improvements can be possible by means of applying Particle-Swarm-Optimization ('PSO') with proposed FBeeAdHoc algorithm to improve the malicious node finding possibilities and improving the time efficiency [13].

Dual-Authentication and Key-Management schemes-for secure-data-transmission in VANET - Vijayakumar P, Azees M, Kannan A, Jegatha Deborah L - 2015 [14]. This paper mainly discusses about the security principles by means of dual-authentication and security key-management principles. For dual-authentication the authors used hash-code security and fingerprint-scanning process, which reduces the possibility for attack with malicious nature. And the total work is based on VANET' environment and provide support to vehicular-communication-model. The group keying model is used to provide enhanced security to the nodes to make proper communication between others. The main-benefit of’ this proposed-system is: Security, which is established in two ways such as authentication and keying. The major drawback found in this work is missing of location-privacy, so that the hackers/intruders can easily get to know regarding vehicle's-location and then the possibility of attack is more in it, so that further implementation logics are required to improve the proposed methodology to work in robust manner [14].

Dynamic-fuzzy-logic-and-reinforcement-learning-for-adaptive energy-efficient-routing in MANET - Saloua.C', Salim.C' - 2016 [15]. This paper concentrates on energy efficiency with successful packet delivery and throughput-improvements. The major algorithm considered into this paper is Dynamic-Fuzzy-Energy-State-AODV ('DFES-AODV'), which enables the routing process based on route-request and route-response principles. The node-lifetime management with energy-efficiency is the major norm deals with this paper and the highlighting term in this-system-is energy-sufficiency to all nodes over communication with other nodes in the mobile-ad-hoc-network environment. The main-benefit of’ this proposed-system is: energy-efficiency and the algorithm processing time is less compare to other similar implementations [7][8][9]. The major drawback found in this work is however it process the routing principles via route-request and route-response strategies, but the limitations and restrictions are high over practical implementations over mobile-ad-hoc-networks [15].

Fuzzy-logic based-unequal-clustering for WSN - Logambigai.R', Kannan.A' - 2016 [16]. The main consideration of this system-is: utilization-of-energy and overall-network-lifetime, which is the major concern and it usually affects based on the arrangement of node over the network environment and the improper operations of wireless-sensor-network such as node-failures due to bandwidth insufficiency. In this work, cluster based arrangements are followed; sink-selection and cluster-head-selection principles are used to provide proper network node arrangements and positioning. The main algorithm implemented into-this paper is: EAUCF, which is derived from the classical routing-algorithm called LEACH and the implementation is done by using MATLAB simulation [16]. Fuzzy based implementation logic guarantee the better network-performance and time-management over network data-transmissions. The main advantage proposed from this paper is the reduction of energy-consumption and lifetime-improvements. And the limitation falls into the work is practical implementation possibilities because of cost and logical problems [16].

Real-time-routing process-for mobile-ad-hoc-network using reinforcement-learning with heuristic-algorithms - Ghaffari A - 2017 [17]. A reinforcement-learning based network performance improvement scheme is discussed in this paper [17]. It has no-assumptions, which are all practically tested and proven results are attained over implementations, which mainly concentrates on packet-delivery-ratio as-well-as reduces the network delay during communications. The main algorithm used in-this-system-is' called Q-learning-Algorithm, which provides better results to attain high packet-delivery-ratio as-well-as the simulation is done by using OPNET/MATLAB environments. The main advantage presented in this-approach-is-improvement of packet-delivery-ratio as-well-as network-lifetime-enhancements and clustering logics are also used in this implementation [17]. The drawback found in the-system-is' restriction over node formation and packet transmission interval is more compare to previous works [5][6].

Novel-trust-framework for VANET - Ahmed.S', Al-Rubeaai.S', Tepe.K' - 2017 [18]. In this paper, Dedicated-Short-Range-Communication ('DSRC') is implemented for Vehicle-to-Vehicle ('V2V') Communications, which is used to identify the malicious activities over the vehicular network environment and raising-report against the misbehaving-node into-the network-environment immediately-to-receiver [18]. All the nodes presented into the network are differentiated under two categories such as trust-values and report-events, generally it is coming under two modes such as true or false. The work is based on the inclusion of trust and receiver recommendations, so that the communication is better than the classical vehicular network communication models. The major benefit of this proposed-system is: robustness and attack finding nature over vehicular network environment and the disadvantage found in this work is conflict occurrence during collaboration-attack models and it is not considering over the implementation as well as this is highlighting in the paper's future scope also [18].

An intelligent-secured and 'energy-efficient-routing-algorithm' for MANET's - Muthurajkumar S, Ganapathy S, Vijayalakshmi M, Kannan A - 2017 [19]. The main consideration of-this-system' falls into two different mobile-ad-hoc-network strategies such as energy and security. All network environments handles and spends more time to preserve the energy level during communication, similarly in this work, the main concentration is for energy-preservation and the security formulations over communication. The main algorithm called Cluster-based-Energy-Efficient-Secure-Routing-Algorithm ('CEESRA') is implemented to provide energy-efficiency and eliminates the possibilities for DoS type of attacks. The main advantage presented in the-system-is' improvement of energy-efficiency and reduces the energy-consumption and security improvements. The main disadvantage handles in this work is trust-inefficiency, so that the paper further enhancement section speaks about that and by applying the fuzzy principles we can get better trustworthy network compare to the present scheme CEESRA [19].

Novel-fuzzy-clustering process for 3D-WSN - Hai DT, Le Vinh T - 2017 [20]. This paper considers the problem occured in wireless-sensor-network clustering principles and 3D-terrains and results with fuzzy-clustering norms to improve the energy over network environment. The main algorithm discussed in the-work-is' Fuzzy-C-Means-3 (FCM3), which covers the problem of Clustering over the wireless-sensor-network and eliminates the energy mismatching problems occured during communication time. The main advantage found in this-work-is' such as dealing the entire work with Three dimensional-Wireless-Sensor-Network ('3D-WSN') and provide decent solutions to all energy oriented problems over WSN. The main limitation found in this work is in two diversities such as number of CH-formation and network-relay problem [20].

III. SYSTEM ANALYSIS & RESULTS

A. Existing System

The past system several researchers proposed several techniques to solve the malicious node issues and trying to improve the energy efficiency over the Mobile-Ad-Hoc-Network environment, however, all are stucked up in certain level of implementations and facing lots of issues over results. Normally a sink oriented route-establishments [2][5][13] are handled for network lifetime improvements, but all those sink-establishments cause time-consumption problem during large coverage distance. So that condition is not a proper solution to solve the issue of network-lifetime enhancements [15][16]. The turst-estimation of nodes are usually happened via its behavioral oriented things such as movement-duration, mobility-interval, packet-transmission strength and etc., but the traditional routing-protocols [8] mainly concentrate on node-mobility alone to perform communications. In this case, the node-failure can happen and it affects the total network at any particular point-of-time. In 2016, Logambigai.R' and Kannan.A' [16] find out the logical and cost expensive problems over their result and they are basically applying the algorithm called EAUCF in their research and get stucked with that point. In 2015, the authors Haddadou.N', Rachedi.A' and Ghamri-Doudane Y, provides the solution to eliminate the-cost-expensiveness as-well-as find-out the-misbehavior-node effectively and the disadvantage found in the work is limited range of data transmission and low data rate over network environments.

Disadvantages Of Existing System

The major disadvantages of existing system are

- Poor in Performance.
- Cost wise Expensive and End-to-End Delay occurs.
- Long-range Mobility issues.
- Node and Network Failures.
- Energy Lacking.
- Poor Coverage and Weak Signal.

B. Proposed System

The following description clearly illustrates the solution to the above mentioned problems in past-researches. The main goal of this proposed system is to eliminate the problem in past systems and improve the network performance by enhancing the routing-procedures over MANET-environment. And finding out the malicious nodes in the environment and remove the malicious nodes from communication scenario while data-transaction between nodes. The entire proposed approach genuinely ensures the node lifetime and in which it indirectly improves the network performance and node robustness. The proposed algorithm called Fuzzy Secured Node Selection Routing (FSNSR), guarantees the network lifetime enhancement, energy-efficiency, security and etc. The logic of fuzzy usually improves the result in all applications better than other approaches, in which it behaves like a questioner and answerer. While communication, the fuzzy acts like a questioner and enquire regarding the next neighbor node and its characteristics by means of raising the Route-Request and waiting for the response from the respective node. The respective neighbor can response only if it has the sufficient energy and has a proper node-identity. If it fails to response, then immediately that particular node will be marked as a malicious node, the next nearest neighbor will be taken-into consideration and repeating the same process until the data reached the receiver-end. So, that the proposed algorithm assures there will be no lacking in network performance as-well-as the security issues caused by hackers/intruders over the mobile-ad-hoc-network environment.

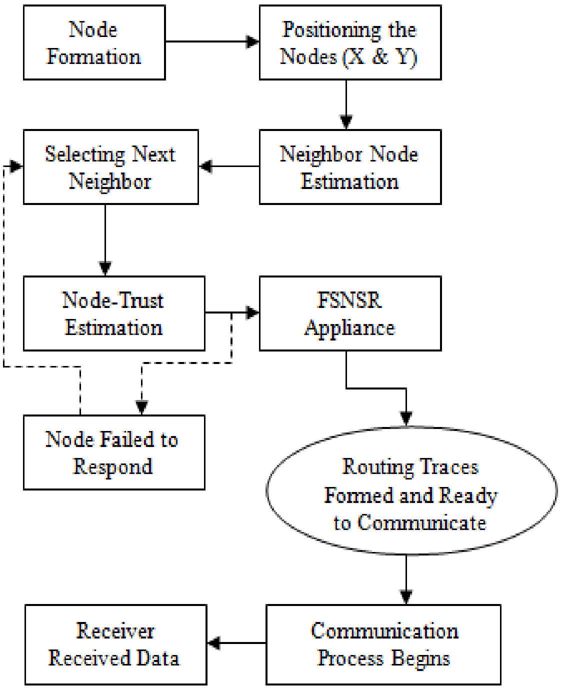

Fig.1 Proposed System Flow Diagram Replication

Advantages Of Proposed System

The major advantages of proposed system are

- Overall Network-Performance Improved.
- Cost effective communication process.
- Intelligent, Compact and faster network connectivity.
- Long Coverage Range.
- Energy Efficiency.
- Signal Strength is high.
- Throughput and Delay improvements.

IV. CONCLUSION

The issues faced in existing system is easily resolved via the proposed suggestions with the help of newly introduced algorithm called Fuzzy Secured Node Selection Routing (FSNSR), which efficiently identifies the malicious nodes and prevent the network from harmful attacks as-well-as intruders/hackers. This FSNSR algorithm provides energy efficiency as well in terms of improving the network performance and lifetime, so that the source and destination can communicate effectively without any network issues. The nodes are considered as two modes such as trusted and untrusted, the trusted nodes are allowed to communicate further to carry the process and the untrusted nodes are marked as 0 in simulation and it will not allowed to communicate further in the mobile network scenario. By using the application of fuzzy the entire work is more sophisticated and flaw free, so that the result occurred from this algorithm is also fault-tolerant and effective in nature. This proposed algorithm guarantees the throughput improvements, energy-efficiency, delay reduction and the packet-delivery-ratio with fault/malicious free nature. In future, the proposed work will be converted using Dynamic-Source-Routing (DSR) protocol, to improve the path-efficiency such as providing the multi-path routing skills to the present scenario to make the network more perfect and works in fine manner.

REFERENCES

1 Chlamtac I, Conti M, Liu JJN (2003) Mobile ad hoc networking: imperatives and challenges. Ad Hoc Netw 1(1):13–64
2 Murthy CSR, Manoj BS (2004) Ad hoc wireless networks: architectures and protocols. Prentice Hall
3 Perkins CE (2001) Ad hoc networking: an introduction. Ad hoc networking, pp 20–22
4 Cho JH, Swami A, Chen IR (2011) A survey on trust management for mobile ad hoc networks. IEEE Commun Surv Tutorials 13(4): 562–583
5 Azzedin F, Ridha A, Rizvi A (2007) Fuzzy trust for peer-to-peer based systems. World academy of science. Eng Technol 21:123–127
6 Perkins CE, Royer EM (1999) Ad-hoc on-demand distance vector routing. In: Proceedings of second IEEE workshop on mobile computing systems and applications (WMCSA'99), New Orleans, pp 90–100
7 Basu P, Khan N, Little TDC (2001) A mobility based metric for clustering in Mobile ad hoc networks. In IEEE Workshop on Wireless Networks and Mobile Computing, 413–418
8 SuW, Lee SJ, GerlaM(2001) Mobility prediction and routing in ad hoc wireless networks. Int J Netw Manag 11(1):3–30
9 Li X, Jia Z, Zhang P, Zhang R, Wang H (2010) Trust-based ondemandmultipath routing inmobile ad hoc networks. IET Inf Secur 4(4):212–232

10 Chiang CC, Wu HK, Liu W, Gerla M (1997) Routing in clustered multihop, mobile wireless networks with fading channel, In IEEE Singapore international conference on networks, SICON'97, April 16–17, 1997, Singapore, pp. 197–211

11 Kumar K, Singh V (2014) Power consumption based simulation model for mobile ad-hoc network. Wirel Pers Commun 77:1437–1448

12 Haddadou N, Rachedi A, Ghamri-Doudane Y (2015) A job market signaling scheme for incentive and trust management in vehicular ad hoc networks. IEEE Trans Veh Technol 64(8):3657–3674

13 Rafsanjani MK, Fatemidokht H (2015) FBeeAdHoc: a secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs. AEU Int J Electron Commun 69(11):1613–1621

14 Vijayakumar P, Azees M, Kannan A, Jegatha Deborah L (2015) Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Trans Intell Transp Syst 17(4):1015–1028

15 Saloua C, Salim C (2016) Dynamic fuzzy logic and reinforcement learning for adaptive energy efficient routing in mobile ad-hoc networks. Appl Soft Comput 38:321–328

16 Logambigai R, Kannan A (2016) Fuzzy logic based unequal clustering for wireless sensor networks. Wirel Netw 22(3):945–957

17 Ghaffari A (2017) Real-time routing algorithm for mobile ad hoc networks using reinforcement learning and heuristic algorithms. Wirel Netw 23:1613–1621

18 Ahmed S, Al-Rubeaai S, Tepe K (2017) Novel trust framework for vehicular networks. IEEE Trans Veh Technol 66(10):9498–9511

19 Muthurajkumar S, Ganapathy S, Vijayalakshmi M, Kannan A (2017) An intelligent secured and energy efficient routing algorithm for MANETs. Wirel Pers Commun 96(2):1753–1769

20 Hai DT, Le Vinh T (2017) Novel fuzzy clustering scheme for 3D wireless sensor networks. Appl Soft Comput 54:141–149

21 Marti S, Giuli T, Lai K, Baker M (2000) Mitigating routing misbehavior in Mobile ad hoc networks. Proceedings of Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 255–265

22 Pappadimitratos P, Haas ZJ (2006) Secure data communication in Mobile ad hoc networks. IEEE J Sel Areas Commun 24(2):343–356

23 Govindan K, Mohapatra P (2011) Trust computations and trust dynamics in mobile ad hoc networks: a survey. IEEE Commun Surv Tutorials 99:1–20

24 Esch J (2010)A survey of trust and reputation management systems in wireless communications. Proc IEEE 98(10):1755–1772

25 Momani M, Challa S (2010) Survey of trust models in different network domains. Int J Ad Hoc Sensor Ubiquitous Comput 1(3): 1–19

26 Ramana KS, Chari A, Kasiviswanth N (2010) A survey on trust management for mobile adhoc networks. Int J Netw Secur Appl 13(4):562–583

27 Abusalah LA (2008) Khokhar, Guizani, M.: survey of secure Mobile ad hoc routing protocols. IEEE Commun Surv Tutorials 19(4):78–93

28 Moe MEG, Helvik BE, Knapskog SJ (2008) TSR: trust-based secure MANET routing using HMMs. Proceedings of ACM Symposium on QoS and Security for Wireless and Mobile Networks, pp83–90

29 Luo J, Liu X, Fan M (2009) A trust model based on fuzzy recommendation for mobile ad-hoc networks. Comput Netw 53(14): 2396–2407

30 Kulothungan K, Angel Arul Jothi J, Kannan A (2011) An adaptive fault tolerant routing protocol with error reporting scheme for wireless sensor networks. Eur J Sci Res 16(1):19–32

31 Ren J, Zhang Y, Zhang K, Shen XS (2014) Exploiting channelaware reputation system against selective forwarding attacks in WSNs. In Proceedings of IEEE GLOBECOM, pp. 330–335

32 Ren J, Zhang Y, Zhang K, Shen X (2016) Adaptive and channelaware detection of selective forwarding attacks in wireless sensor networks. IEEE Trans Wirel Commun 15(5):3718–3731

33 Ren J, Zhang Y, Zhang K, Shen XS (2015) SACRM: social aware crowdsourcing with reputation management in mobile sensing. Comput Commun 65:55–65

34 Bao F, Chen R, Chang M, Cho JH (2012) Hierarchical trust management for wireless sensor networks and its applications to

35 trustbased routing and intrusion detection. IEEE Trans Netw Serv Manage 9(2):169–183

36 Li R, Li J, Liu P, Chen H (2007) An objective trust management framework for mobile ad hoc networks. Proceedings of IEEE vehicular technology conference, pp. 55–60

37 Jerusha S, Kulothungan K, Kannan A (2012) Location aware cluster based routing in wireless sensor networks. International Journal of Computer & Communication Technology 3(5):1–6

38 Zhang DG (2015) Extended AODV routing method based on distributed minimum transmission (DMT) for WSN. Int J Electron Commun 69(1):371–381

39 Zhang DG, Li G, Zheng K (2014) An energy-balanced routing method based on forward-aware factor for wireless sensor network. IEEE Trans Ind Inf 10(1):766–773

40 Zhang DG, Zheng K, Zhang T (2015) A novel multicast routing method with minimum transmission for WSN of cloud computing service. Soft Comput 19(7):1817–1827

41 Zhang D, Wang X, Song X (2015) New clustering routing method based on PECE for WSN. EURASIP J Wirel Commun Netw 2015(162):1–13

42 Zhang DG, Zhu YN (2012) A new constructing approach for a weighted topology of wireless sensor networks based on localworld theory for the internet of things (IOT). Comput Math Appl 64(5):1044–1055

43 Liu S, Zhang T (2017) Novel unequal clustering routing protocol considering energy balancing based on Network Partition & Distance for Mobile education. J Netw Comput Appl 88(15): 1–9

44 Zhang DG, Niu HL, Liu S (2017) Novel PEECR-based clustering routing approach. Soft Comput 21(24):7313–7323

45 Zhang DG, Ge H, Zhang T (2018) New multi-hop clustering algorithm for vehicular ad hoc networks. IEEE Trans Intell Transp Syst 7:1–14

46 Zhang T, Dong Y (2018) Novel optimized link state routing protocol based on quantum genetic strategy for Mobile learning. J Netw Comput Appl 122(15):37–49

47 Liu S, Liu XH (2018) Novel dynamic source routing protocol (DSR) based on genetic algorithm-bacterial foraging optimization (GA-BFO). Int J Commun Syst 13(8):1–15

AUTHORS PROFILE

Rajkumar.K Research Scholar, Dept. of Computer Science and Engineering , Noorul islam Centre for Higher Education, Kumaracoil-629180, Tamilnad,India.

Dr.M.K.Jeyakumar Professor, Dept. of Computer Applications, Noorul islam Centre for Higher Education, Kumaracoil-629180, Tamilnadu.India.