A BPR based Routing in Presence of Selfish Nodes for MANET

[1]M. Kaveri [2]S. Ramesh
[1]Student [2]Assistant Professor
[1,2,3,4]Department of Information Technology
[1,2]K.L.N College of Engineering

Abstract

Mobile Ad-hoc Networks (MANETs) is self-configured and decentralized wireless network without any prior infrastructure. Every node in it acts as a router as well as end system and hence each node in MANET is allowed to move freely which makes routing difficult. Most of the MANET routing algorithms like AODV and DSR assume that every node will forward every packet it receives. In opportunistic routing, a node selects and prioritizes multiple nodes which can act as potential packet forwarders. Source node will relay packets to the destination node through the intermediate node. However, misbehavior of the selfish nodes is a common phenomenon in MANET. These nodes use the network and its services and do not provide any services to intermediate nodes in order to save energy such as battery, CPU Power and bandwidth for relaying data from other nodes and reserve for themselves. These selfish nodes will degrade the performances of wireless ad hoc networks. In this thesis, Using OR and BPR routing protocols to overcome the presence of selfish nodes and also BPR routing protocol used to avoid malicious nodes. These protocols used to avoid congestion and perform the simulation using Network Simulator.
Keyword- MANETs, Selfish nodes, BPR, Opportunistic Routing, Routing Protocols-AODV

I. INTRODUCTION

Routing is a fundamental operation in mobile ad hoc network. Lack of infrastructure, dynamic links, and broadcast nature of the communication makes routing in MANET a challenging problem. Traditional routing protocols for MANET like AODV [1], DSR [2], AOMDV [3] perform best path routing, which work similar to routing in the wired networks. Best path routing selects the best neighbour from each hop to forward a packet. This strategy has limitations in dynamic wireless environment due to volatility of transmission links between the nodes. A distinctive feature of wireless communication is the broadcast nature. When a node sends a packet to its neighbour, each one-hop neighbour listens the packet. As it causes interference with other communications, this is considered as a disadvantage in traditional routing protocols. Opportunistic Routing (OR) uses the broadcast nature of the communication by dynamically selecting route to the destination. In OR, each transmission of a packet is for multiple neighbouring nodes. OR considers multiple neighbours as potential candidate nodes, which can forward the packet further toward the destination. The candidate nodes attempt to forward the received packet as per the priority order decided by the previous sender. The OR causes decrease in the number of transmissions required to send a packet from source to the destination [4,5]. Du et al. [6] lists benefits of OR are as follows. OR combine multiple weak links into one strong link. As all possible links within one transmission are considered, OR may use the farthest hop which successfully receives the packet as the next packet forwarder. Hence it can take advantage of unexpectedly long transmissions. Hsu et al. [7] point out that, OR can use backup links and it minimizes transmission failure probability. This improves reliability of the communication. Experiment results in [4] and [8] show that OR has the potential to perform better than traditional routing protocols. MANET routing protocols conventionally assume that, every node participating in the communication is honest and cooperative. This is also applicable to OR protocols. Hence routing is successful only if the participating nodes cooperate with each other. It is impractical to assume that, all nodes participating in the network are cooperative and honest every time. Few nodes participating in the network may be selfish nodes. Selfish nodes drop packets for conserving own battery and processing power, or these nodes are interested to disturb the communication. Few nodes participating in the network may be faulty, which again causes packet drops. Packet dropping attack is a serious issue in MANET routing, and it may result into the collapse of network. Hence designing a routing protocol which can overcome the presence of selfish nodes and improve network performance is important [9]. Using trustworthiness of nodes for decision making in routing has recently gained a large amount of attention. The [10–12] are few trust based routing protocols, which aims at identifying selfish nodes and neutralize their impact in the routing. These algorithms optimize the network performance by utilizing trustworthy nodes in an effective way. The presence of selfish nodes also impact on performance of the OR protocols. However, there is limited work done which addresses the presence of selfish nodes in the OR protocols. The paper proposes a novel trusted OR protocol, which overcomes presence of selfish nodes in the network. The design of the proposed algorithm is inspired from CORMAN [8] and is a vital extension of CORMAN. The algorithm evaluates the path goodness value for each path towards the destination. The path goodness value is derived from trustworthiness of the nodes on the path and proximity of these nodes towards the destination. The

algorithm uses a trust model based on packet forwarding behaviour of the nodes. The path goodness value is used as metric for deciding and prioritizing candidate nodes participating in OR.

II. RELATED WORK

Extremely opportunistic routing (ExOR) [2] protocol is considered as the first OR protocol. In ExOR, a node broadcasts data packets to neighbours for packet delivery to the destination. Each node finds priorities of next potential forwarders and announces these priorities in the broadcasted packet. ExOR uses MAC and routing layer together to avoid transmissions of same packet from multiple nodes. The algorithm imposes strict timing constraints among the forwarders for coordination in the packet relay process. ExOR followed by a number of OR proposals by different researchers in the last decade. OR protocol design research is dominated by two issues. The first one is making proper choice of candidate nodes; and second is improving performance of OR protocols [6]. Candidate selection and ordering help to find the best route. The nodes use different metrics for candidate selection and prioritization. The traditional routing algorithm like AODV, DSR and AOMDV uses hop-count as metric for candidate selection. ExOR [2], and protocols use the Expected Transmission Count (ETX) as a metric for ordering candidate set. In these protocols, sender node prefers a node having minimum ETX towards the destination. The ETX parameter prefers the farthest node as a candidate node. it uses EAX as parameter for choosing the best candidate node to the destination. Another motivation behind the design of OR protocol is to improve reliability or efficiency of routing. Duplicate packet forwarding in OR reduce efficiency as same packet is forwarded by many nodes. [8] propose a Duplicate-Free opportunistic packet forwarding protocol (DFOR). In DFOR forwarding nodes minimize packet broadcasts for each packet.it uses energy-consumption based objective functions (OF) to calculate energy consumption by all nodes on the path to the destination. The uses information exchange at physical, MAC and network layer for OF calculation. Each node trying to find the best node for packet forwarding causes heavy computational overhead in working of OR [1]. CORP-M [1] do not use the pre-selected list of potential forwarders. The protocol divides the network into different regions by allowing a node to calculate its own region. Then these regions are taken into consideration for packet forwarding.

The secure routing algorithm in MANET uses cryptography or trust based mechanisms for improving security of communication. Both approaches have their own merits and limitations. Few examples of MANET routing protocol using cryptography is SDMP [10]. Cryptographic methods need pre-establishment of the keys between the nodes participating in communication. So it may require setting up a Certificate Authority or a Key Distribution Centre for authentication and secure key distribution. This is practically difficult to implement in an open ad hoc network wherein single administrative control is not available on all participating nodes. Cryptographic methods used in MANET routing protocols have more computational overhead as compared to trust based approaches. In MANET, a node may start misbehaving after passing cryptographic security checks. The security attacks pertaining to node behaviours can be successfully detected and prevented using trust.

The trust management mechanism is useful for identifying selfish nodes and minimizing their impact on the communication. Few examples of such trust based routing protocols are: AOTDV [13], FTDSR [12], and CTrust [14]. AOTDV [13] is a trusted extension of ad hoc on-demand multipath distance vector (AOMDV) routing protocol. The protocol discovers multiple paths from source to destination on the basis of two parameters: hop counts and trust values. In FTDSR [12], authors have extended standard reactive routing protocol viz. Dynamic Source Routing (DSR) protocol. The algorithm isolates untrustworthy nodes from the network and finds reliable route. The authors have used fuzzy logic and analytic hierarchical processing for deriving trust values of the nodes. Zhao et al. [13] have devised trust model for cyclic MANET (cMANET) to handle trust establishment and aggregation. Trust model in MANET considers the neighbour trust along with time and location.

MCOR [14] is the first scheme which addresses the presence of selfish nodes in OR. In MCOR, each node calculates trust for neighbour nodes according to interactions with that node in the past. MCOR uses trust degree as the parameter for filtering selfish nodes from being forwarder. The MCOR algorithm uses distance from a node to the destination as metric to determine the best candidate nodes. The ORPSN algorithm differs with MCOR on following aspects: calculation of trust degree of the neighbour nodes, using trust degree in decision. Making, strategy for choosing best candidate node and coordination amongst the nodes for deciding who will forward the packet. TMCOR [15] is inspired from MCOR. It applies the trust based OR for Vehicular ad hoc Network (VANET).

The design of ORPSN is extended from Cooperative Opportunistic Routing in Mobile ad-hoc Networks (CORMAN) [8]. CORMAN is a network layer OR protocol for mobile ad hoc networks. The design of CORMAN is based on Ex-OR [4], but it extensively uses network layer operations rather than MAC layer.

III. BPR ROUTING PROTOCOL

This section gives an overview of BPR routing protocol at the beginning; then mathematical modeling of the algorithm and protocol design is discussed in details.

A. Protocol Overview

BPR has two primary components viz. candidate selection and coordination method. Though BPR[11] protocol delays the final route selection, it is necessary to nominate proper candidate nodes in advance. Candidate selection component decides and arranges

candidate nodes using path goodness metric. If the selected best candidate node does not respond to packet forwarding then coordination method is useful.

BPR mimics working of CORMAN as follows. It uses strategy similar to Proactive Source Routing (PSR) [16] to build routing tables on each node. The packets are forwarded in the form of batches from upstream nodes (which are closer to the source node) to downstream nodes (which are closer to the destination). The packet contains a forwarder list, which contains ID's of nodes along the route to the destination. The packets from a batch use the same forwarder list. The forwarder list is initially prepared by the source node. When packets move toward the destination, the forwarder list may be modified by intermediate nodes. As the packets are forwarded as per updated route, this information is propagated to upstream nodes. The detailed discussion of BPR candidate selection and coordination method is as below.

The BPR's candidate selection component is responsible for choosing candidates and ordering them as per priority according to the path goodness metric. The path goodness value is calculated for each path from source to destination using trustworthiness of nodes lying on the path and proximity of these nodes to the destination. BPR candidate order is global; it means that while choosing candidate order all intermediate nodes on the path to the destination are considered.

Each node calculates trustworthiness of its neighbour nodes depending on past behaviour of the node. The nodes passively monitor behaviour of their neighbours. The node records positive and negative observations of its neighbours and uses Bayesian inference to calculate the trust value. The path trust of each route toward the destination is calculated using trust values of nodes lying in the path to destination. It also considers proximity of the node to the destination for choosing it as a candidate node. It measures the proximity of the node to the destination in the form of estimated transmission count (ETX). Each node calculates ETX towards the destination and shares it with its neighbours.

The path goodness value is a weighted combination of path trust and ETX values. Path goodness value is used to decide the best path toward the destination. BPR builds routing table using path goodness values. Each node keeps information of two best paths to the destination in its routing table using two highest priority candidate nodes.

After data packet broadcasts, candidates will respond in the order, i.e. next expected forwarder followed by second best forwarder. The coordination method takes care about this. It uses timer based coordination method similar to ExOR [4] and CORMAN [8]. After receiving a packet, the selected next expected forwarder forwards the packet further. Second best forwarder responds only when it does not observe any response from next expected forwarder within a threshold time. In ORPSN, if next expected forwarder fails, then forwarding node declares who will act as second best forwarder. This strategy used by ORPSN and BPR is different from one used by CORMAN. If the next expected forwarder do not respond in time, then the nodes decide the second best forwarder at real time in CORMAN protocol.

B. Mathematical Modelling

The mathematical model for calculating path goodness and packet forwarding process is discussed in detail in this section.

1) Path Goodness Metric

ORPSN and BPR uses trust evaluation based on Bayesian network. A Bayesian network uses Beta distribution and Bayesian inference to determine the trust relationships among the nodes. As only two parameters viz. positive observations u and negative observations v are needed, we have used Beta distributions. The values of u and v are continuously updated as observations are made by the node [17]. Let x and y be two neighbouring nodes in the MANET and there are total n observations node x made about node y. If T new is the probability of positive behaviour by y at n + 1 times, then posterior distribution of positive behaviour of node y is a Beta distribution with the density function as below:

$$Beta(T_{old}|u,v) = \frac{\tau(u+v+2)}{\tau(u+1)\tau(v+1)} {T_{old}}^{u}(1-T_{old})^{v} \qquad (1)$$

$$T_{new} = E(Beta(T_{old}|u+1, v+1)) = \frac{u+1}{u+v+2}$$

$$\text{where } 0 < T_{old} < 1, \quad 0 < T_{new} < 1 \quad and \quad \text{u, v} > 0 \qquad (2)$$

The trust value of the path is computed using trust values of nodes along the path. ORPSN considers that, the path trust is not more than the trust value of most unreliable intermediate node on the path. ORPSN calculates the path trust denoted by MPT as below:

$$MPT = Min(\{T_{j,k}|n_j, n_k \text{ belong to path and } n_j \rightarrow n_k \text{ and } n_k \neq destination\}) \qquad (3)$$

In above equation n j and nk are any two adjacent nodes on the path.

The ETX value is calculated for each neighbor with respect to the destination. The ETX represents node's proximity to the destination [4]. Each node shares ETX values with its neighbors. The path goodness value for node s to d using m as next hop is calculated as below:

$$Path\ Goodness_{s,d,m} = \alpha * \left(\frac{1}{ETX_{s,d,m}}\right) + \beta * MPT_{s,d,m}$$

$$here\ m \in Neighbor\ set\ of\ s; if\ m = d\ then\ MPT_{s,d,m} = 1 \qquad (4)$$

IV. BPR ROUTING ALGORITHM

This section discusses various algorithms used by ORPSN. Then data structures and packet format used by the ORPSN protocol is discussed in details. An illustrative example describing working of candidate selection in ORPSN is given at the end of the section.

A. Routing Algorithms

In Algorithm 1, node s wants to choose its candidate nodes viz. next expected forwarder and second best forwarder to reach the destination d. It starts by creating an initial candidate set. A neighbor m of s is included in the initial candidate set only if ETX(m,d) < ETX(s,d). Thus ORPSN filters out certain neighbors being potential candidates. It ensures that, packet always moves in the forward direction toward the destination. After filtration newly generated candidate set is a subset of the initial candidate set. All nodes which are part of the candidate set must select their candidate sets first. This is done by recursively applying candidate selection algorithm. Finally, node s selects the best two candidate nodes from shortlisted candidate nodes using path goodness value. The candidate selection algorithm is continuously updating next expected forwarder and second best forwarder nodes with respect to each destination. The algorithm puts updated information in routing table of the node.

Algorithm 1 : Candidate node selection (s,d)
$CandidateSet_{s,d} \leftarrow \phi$
If s == d then
    $PathGoodness(s, d) \leftarrow 0$
    flag(s) = TRUE
    Return
End if
$InitialCandidateSet_{s,d} \leftarrow \phi$
For all $m \in NeighborSet(s)$ do
    If ETX(m,d) < ETX(s,d)
        $InitialCandidateSet_{s,d} \leftarrow InitialCandidateSet_{s,d} \cup \{m\}$
    End if
End for
For all $m \in InitialCandidateSet_{s,d}$ do
    If (flag(m) == FALSE) then
        Call Candidate node selection(m,d)
    End if
End for
For all $m \in InitialCandidateSet_{s,d}$ do
    Find $PathGoodness(s, d, CandidateSet_{s,d} \cup m)$
    flag(s) = TRUE
End for
Sort nodes from CandidateSet as per path goodness values.
Return first two candidates viz. next expected forwarder and
second best forwarder from Candidate Set.

Algorithm 2 updates ETX value of each node toward the destination. Each node periodically sends probe hello messages and determines link delivery probability (LDP) with each of its neighbor. The link ETX i.e. ETL is calculated using LDP. The nodes share ETX values for each destination after periodic intervals.

Algorithm 2: Update ETX (Estimated Transmission Count)
At a periodic interval update link delivery probabilities with all neighbor nodes
    using probe Hello packet
Update ETL i.e. link ETX value for each neighbor. ETL = 1/link delivery probability
Update ETX value for each destination. ETX = Sum of Link ETX values along
    lowest ETX path to the destination

V. EXPERIMENTAL RESULTS

In this section, to evaluate the performance of BPR through NS-2 simulations using some pre-defined metrics. To rate the performance, we compare the performance of our result with BPR and ORPSN approaches using the configuration setup shown in

Table 1. Our simulation is based on a configuration where 50 to 100 nodes, are randomly scattered in a monitored region of 1,000 m 1,000 m. The sensor nodes perform continuous information sensing while sending periodic updates to the sink node.

A. Experimental Setup

The NS-2.34 [5] simulator is used to evaluate the performance of BPR, ORPSN, AODV [1], DSR [2], and CORMAN [8] routing protocols. The IEEE 802.11 extension distributed coordination function is used for wireless networks .We spread 50 nodes at random positions; each node having the transmission radius of 250m within a rectangular field. The node mobility uses the random waypoint model. The nodes use 10 s pause time .We evaluated performance of the protocols under various test conditions. The test conditions used are varying grid size, varying node speed and varying number of selfish nodes.

B. Simulation Parameters

Parameter	Value
Simulation time	500 s
Number of nodes	50
Grid size (variable in test condition 1)	500, 600, 700, 800, 900, 1,000 in m^2
Mobility model	Random way point
Traffic type	Constant bit rate (CBR) UDP
Transmission radius	250 m
Packet size	512 bytes
Connection rate	50 packets/s
Connections	5
Pause time	10 s
Speed (variable in test condition 2)	0.5, 4, 8, 12, 16, 20 in m/s
Propagation model	Two ray ground
Number of selfish nodes (variable in test condition 3)	0, 3, 6, 9, 12

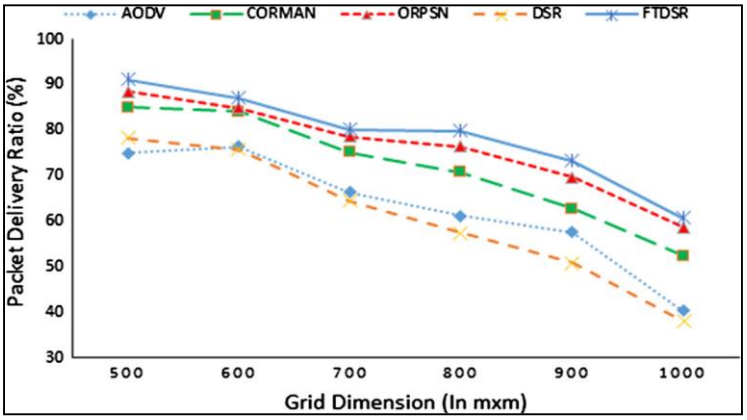

Fig. 5.1: Measurement of packet delivery ratio by varying grid dimensions

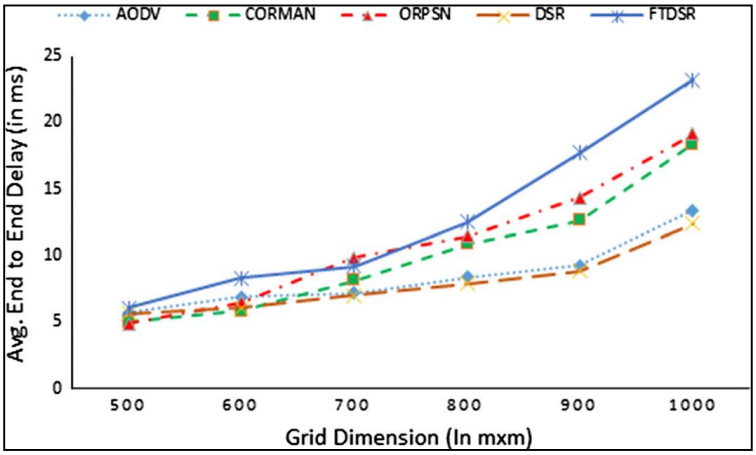

Fig. 5.2: Measurement of avg. end to end delay by varying grid dimensions

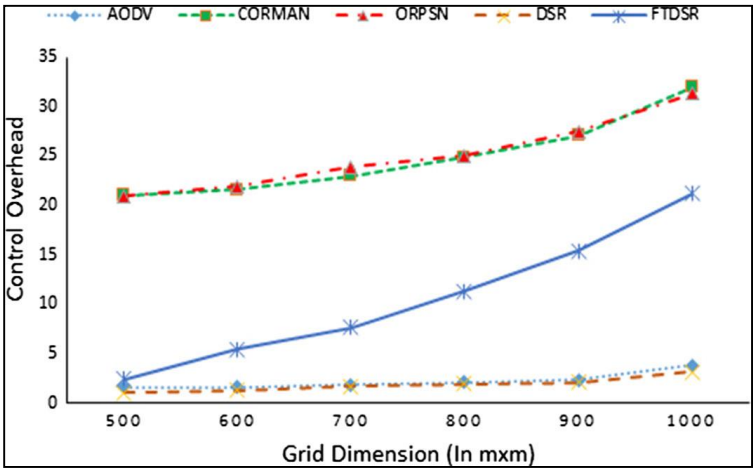

Fig. 5.3: Measurement of control overhead by varying grid dimensions

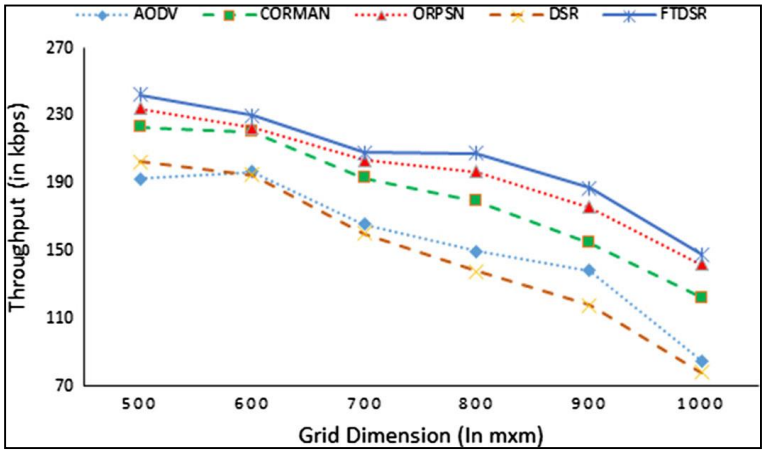

Fig. 5.4: Measurement of throughput by varying grid dimensions

VI. DISCUSSIONS

A. Immunity against Selfish Nodes

Experimental results show that, BPR protocols viz. ORPSN and CORMAN have better immunity against selfish nodes attack as compared with traditional reactive routing protocols like AODV and DSR. In BPR a set of candidate nodes can potentially act as packet forwarders. The candidate nodes respond to the packet forwarding as per priority decided by the original sender. If the high priority candidate does not forward the packet, next candidate node attempts packet forwarding. This continues until at least one

candidate forward the packet. This improves reliability of packet delivery in BPR. CORMAN takes care of packet drops by selfish nodes up to a certain extent and it has a better resilience to presence of selfish nodes in the network as compared to AODV and DSR. However, CORMAN chooses the candidate nodes depending on hop count and ETX, which may result into choosing a selfish node as *next expected forwarder* or s*econd best forwarder*. To sum up, PDR of CORMAN is more than AODV and DSR but BPR performs better.

B. Attack and Trust Model

BPR assumes simple attack model; wherein selfish nodes simply drop the packets. The trust model adopted in this paper uses packet forwarding behavior of the nodes to decide trustworthiness. However, there are several ways through which malicious nodes can disrupt the network operations. Though trust management systems are useful for improving security in the MANET, it can be attacked. it have discussed possible attacks on the trust schemes in MANETs. The [19] gives hints about the secure and robust design of a trust management system. A more complex trust model can be developed, which addresses sophisticated attacks on network operation and attack against the trust management systems.

VII. CONCLUSION

BPR makes ingenious use of the broadcast nature of wireless communications for routing. The issues like security and presence of selfish nodes are not yet addressed much in the context of BPR protocols. This paper introduced a novel trusted BPR protocol, which selects the candidate nodes using trust and path optimality. BPR extends ORPSN and CORMAN functionality to neutralize the presence of selfish nodes in the network. BPR uses a new metric viz. path goodness to decide optimal forwarder for delivering the packet to the destination. In BPR, source node establishes a trustworthy and optimal path to a destination by selecting the best candidate nodes at each stage in route discovery. BPR also replaces the strategy used by CORMAN for selecting second best forwarder. The future extensions to this work may address malicious nodes, which are capable of making complex attacks in the network operation. Our forthcoming plan includes refining the trust model to make it robust against attacks on itself. We believe that, trust may be useful for decision making at various stages in BPR.

REFERENCES

[1] Ajmal, M. M., Madani, S. A., Maqsood, T., Bilal, K., Nazir, B., & Hayat, K. (2013). Coordinated opportunistic routing protocol for wireless mesh networks. Computers & Electrical Engineering, ISSN 0045–7906, 39(8), 2442–2453.
[2] Biswas, S., & Morris, R. (2009). ExOR: Opportunistic multi-hop routing for wireless networks. In Proceedings of conference on applications, technologies, architectures, and protocols for computer communications.(SIGCOMM ’05), ACM, New York, NY, USA, pp. 133–144.
[3] Bo, W., Chuanhe, H., Layuan, L., & Wenzhong, Y. (2011). Trust-based minimum cost opportunistic routing for ad hoc networks. Journal of Systems and Software, 84(12), 2107–2122, ISSN 0164-1212
[4] Hsu, C.-J., Liu, H.-I., &Seah,W. K. G. (2011). Opportunistic routing: A review and the challenges ahead. Computer Networks, ISSN 1389–1286, 55(15), 3592–3603
[5] http://www.isi.edu/nsnam/ns/.
[6] Li, X., Jia, Z., Zhang, P., Zhang, R., & Wang, H. (2010). Trust-based on-demand multipath routing in mobile ad hoc networks. IET Information Security, 4(4), 212–232.
[7] Li, F., & Jie,W. (2010). Uncertainty modeling and reduction in MANETs. IEEE Transactions on Mobile Computing, 9(7), 1035–1048.
[8] Liu, H., Zhang, B., Mouftah, H. T., Shen, X., & Ma, J. (2009). Opportunistic routing for Wireless ad hoc and sensor networks: Present and future directions Myung, J., & Lee, W. (2012). Eliminating duplicate forwarding in wireless opportunistic routing. IEEE Communications Letters, 16(4), 510–513.
[9] Myung, J., & Lee, W. (2012). Eliminating duplicate forwarding in wireless opportunistic routing.
[10] Martin Schutte (2006). Detecting Selfish and Malicious Nodes In MANETs.
[11] Naimah Yaakob, Ibrahim Khalil, Heshan Kumarage, Mohammed Atiquzzama, and Zahir Tari, IEEE(2015).By-Passing Infected Areas in Wireless Sensor Networks Using BPR. IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 6.
[12] Othmana, J. B., & Mokdadb, L. (2012). Enhancing data security in ad hoc networks based on multipath routing. Elsevier Journal of Parallel Distributed Computing, 70, 309–316.
[13] Perkins, C.E., & Royer, E. M. (2013). Ad hoc on-demand distance vector routing. In Proceedings of workshop mobile computing systems and applications.
[14] Sun, Y., Han, Z., & Liu, K. J. R. (2008). Defense of trust management vulnerabilities in distributed networks. IEEE Communications Magazine, 46(2), 112–119
[15] Wang, Z., Chen, Y., & Li, C. (2012). CORMAN: A novel cooperative opportunistic routing scheme in mobile ad hoc networks.
[16] Wang, Z., Chen, Y., & Li, C. (2014). PSR: A lightweight proactive source routing protocol for mobile ad hoc networks. IEEE Transactions on Vehicular Technology, 63(2), 859–868.

[17] Xia, H., Jia, Z., Ju, L., & Zhu, Y. (2011).Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory. IET Wireless Sensor Systems, 1(4), 248-266.
[18] Zhao, H., Yang, X., & Li, X. (2013). Trust management in cyclic mobile ad hoc networks. IEEE Transactions on Vehicular Technology, 62(6), 2792–2806.
[19] Zhizhong, J., Chuanhe, H., Liya, X., Bo, W., Xi, C., & Xiying, F. (2012, October). A trusted opportunistic routing algorithm for VANET. In Third International Conference on Networking and Distributed Computing (ICNDC), pp. 86–90.