Node Activities Learning (NAL)Approach to Build Secure and Privacy-Preserving Routing in Wireless Sensor Networks

K. Ramesh Rao[1], S. N. Tirumala Rao[2,] and P. Chenna Reddy[3]

[1]Research Scholar, CSE, JNTUA, Anantapuramu (A.P), India
[2]Professor, Dept. of CSE, NarasaraoPeta Engineering College, Narasaraopeta, Guntur (A.P), India
[3]Professor, Dept. of CSE, JNTUA, Anantapuramu (A.P), India

Abstract: Wireless networks are becoming the most popular in today communication systems, where users prefer to have wireless connectivity regardless of its geographic location. But the open environment of wireless communication increasing threat on the wireless networks under diverse network circumstances. The random and dynamic activity increases the vulnerability due to the complete dependency on the intermediate nodes which frequently join and leave the network. It is extremely significant to have a secure routing in such a dynamic network to preserve the data privacy. In this paper, we propose a secure and privacy routing based on Node Activities Learning (NAL) approach. This approach knows the runtime activities of the node to predict the probability of activity transformation for the intentional and unintentional activities which interrupt the data communication and affects the privacy. The mean of privacy is decided based on the node individual trust factor. It also suggests a method for the node which loses their trust due to the unintentional activities. A simulation-based evaluation study shows positive improvisation in secure routing in different malicious node environment.

Keywords: Node Activities, Learning, Secure routing, Privacy, Wireless sensor networks, NAL

1. Introduction

The security of wireless networks is of significant concern to the basic functionality of the network. By ensuring that security issues are met, it can ensure the accessibility of network services, the privacy, and reliability of its data. The wireless networks suffer from security attacks as a result of its independent characteristics such as open communication media, dynamic topology changes, lacking any central supervising administration and unstable security mechanisms. These aspects have transformed the defending circumstances of wireless networks not in favor of security threats. The wireless networks function with no central management, where nodes communicate with each other based on communal trust. This feature formulates wireless networks more susceptible to exploitation by an intruder in the network. Wireless connections also make wireless networks further susceptible to attacks making it simpler for the attacker to navigate within the network and to gain admittance to in progress communication [1], [2], [3]. Even the mobile nodes in the wireless range can listen to join the network for creating malicious activities.

The communication protocol used for routing is intended to provide standards that all participants node should comply with the rules. But, in an untrustworthy communication, a malfunctioning node perhaps damages the network performance. Therefore, to make it certain proficient utilization of resources in wireless networks is essential to have trustworthy communication where nodes fully depend on the co-operation of successful packet transmission. Based on the conventional aspect of network securities are mostly dependent on the encryption methods. Unfortunately, these methods are unable to control the malfunctioning on the network. To alleviate such attacks, many researchers have used the concept of behavioral perception depending on observing the behavioral prototypes of neighbor nodes and marking abnormal patterns. The concept of use relates to communication activities such as sending packets or non-communication activities, such as announcing the reported information. The widely used instinct of behavior-based detection is Local Control [4], [5], [6]. In local control surveillance, the nodes monitor some of the traffic that goes in and out of their neighboring nodes.

Selfishness and malicious behavior are categorized into two main categories of medical illness [7], [8], [9], [10]. Selfish nodes constantly put a goal to exploit extra network and device resources or to produce inadvertently incorrect node messages contrast to regular nodes. Generally, selfish nodes obstruct communication channels to lower bandwidth and reduce device energy resources for packet routing. The entire communication behavior has become the target of a malicious node to construct “congestion, denial of service, path fabrication," and so on. If there are malicious nodes of this kind in the network, it creates a serious communication problem and can collapse the network [5], [11], [12].

In this paper, we propose the NAL approach to recognize selfish and malicious nodes utilizing their activities prediction during routing in wireless networks. This issue is addressed in two aspects: 1) Node Activities Learning Method and 2) Secure and Privacy Routing using NAL. The process of NAL is based on a probability of activity transformation prediction and later building a secure route for routing. The build route utilizes to perform the security and privacy routing to eliminate the true malicious or selfish node that influences network reliability and have an effect on trusted nodes. Accurate predictions help ensure to build network nodes reliability and restoring network stability for longer periods and provide better privacy preserving routing.

The remaining paper is organized as follows. Section 2 discusses the related research works, Section-3 present the proposed node activity learning approach and trust prediction for secure routing, in Section 4 the experiment evaluation and result in analysis and finally, Section 5 presents the conclusion of this paper.

2. Related Works

The actively changing topology, distributed operations, and resource limitations are several of the exclusive features found in wireless networks, which amplify the susceptibility of such networks. Several features can be utilized to categorize attacks in wireless networks. Due to the communication environment and its openness, the number of ad hoc routing protocols is a vulnerability [2], [9], [13], [12]. Due to high memory requirements and high-power consumption, the traditional approach to mitigate the security attacks does not apply to wireless networks routing. So far, many "trust management frameworks" and "recognition-based frameworks" have been proposed, using various methods to perform security clarification with low reliability and resource utilization.

Secure routing in wireless networks in different aspect has been extensively studied [14], [15], [16], [17]. However most of the proposals derive the conventional settings of the static or wired networks methods [18], [19], [20], [21], these methods mechanism can mitigate attackers, but they also eliminate the honest nodes for the network. Many reputation-based approaches [22], [23] are vulnerable to voting stuffing, in which a malicious node praises another malicious node or praises a malicious node that implies a legitimate node. All reputation-based approaches are affected by the behavior activity of the nodes that are functioning correctly, but they provide incorrect information about other nodes. Moreover, all these approaches suffer from non-convergence behavior actions. Thus, the reputation state of a good node may remain low, or the reputation state of a malicious node may be misdiagnosed.

R. Hinge et al. [9] proposed an "opinion-based trust model" that operates based on network attributes. In this study, the reliability of the arbitration node can be calculated, and the estimation of the trust value can support the decision on the communication of the specific path. Communication in the wireless networks must be performed through intermediate nodes because of an inadequate radio range. In consequently the malicious nodes be able to connect to the network and destruct the routing procedure. Thus, for a trust assessment process containing at least two values as "negative" and "positive" in the development of discovering for a trusted node. Later obtaining the trust value for the entire node next to the path, can take a view of the neighboring node and perform a path searching process.

A malicious node can recover the consistency of a node by broadcasting a harmful message, while at the same instance delivering a positive message. "Forged message detection" can decrease the number of influenced messages directly or indirectly evaluating the trust schema in the recovery plan. Previous research on trust restoration has been discussed in [24], [25], [26], and node replacement cannot be a significant quantity for node trust revival.

C. E. Xi et al. [27] discusses "Behaviour Feedback (TMS-BF) -based trust management plan" in a nonsensical environment where nodes with low node density and slow-moving nodes cannot effectively utilize the opportunity to achieve self-organizing identity authentication in Network routing. However, in an opportunistic network, there is no need to set up complete mutual authentication for each conversation, assuming most communications originate from delivery operations. Therefore, a new trust management technique is proposed based on the information of behavior feedback to compensate for the insufficiency of identity authentication. By using a supported "certificate chain" based on social characteristics, the mobile node gradually builds up a "local certificate" graph that evaluates the web for "identity trust" relationships. On the other hand, the successor creates a "behavioral trust" relationship for slow-moving nodes by generating an acknowledged feedback packet for each positive action. Simulation results show that implementing a trust system can effectively improve the likelihood of transmission and reliable reconstruction when there are a large number of corrupted nodes and the ability of the trust system.

A "Friend-based ad-hoc routing using Challenges for Security (FACES)" to set up a secure and trustworthy routing in wireless networks is described by SK Dhurandher et al. [13]. It defines a plan for constructing a secure network depending on a group of friends list, where they distribute the group list in the network. Friends are assessed depending on achieving the data transfer among the nodes of previous friends on the network successfully. Every node executes a procedure to periodically retrieve a shared friend list, creating a friend's node's responsibility. The update from the intermediate nodes helps to eliminate the malicious nodes easily from the network. This method does not impose to see adjacent communications for evaluation of node credibility. The disadvantage of this is "delayed from end to end" because of substantial over-the-counter and malicious behavior of a friend's node that affects most listed friends' nodes and also the network steadiness.

Additional trust-based routing approaches are being described in [12], [16], [20], [21]. In these approaches, each node uses the preliminary assessment of the trust as uncertainty and its value is to be informed by the feedback of another node specified from time to time to describe a correlation of trust. The trust-based routing based on the probability of forwarding packets previous suggested in [2]. It determines the "direct trust" of the node with the number of packets they transmit. Each node increases the trust value when it successfully passes the packet and decreases the trust value when deleting the packet. This approach is integrated with the dynamic routing protocol, and trust values are loaded with routing request packets while searching for a route.

Most approaches have been shown to perform calculations independently of the understanding of patterns of activity in past routing, taking into account only the feedback provided by the node. In this paper, we propose a method to construct a secure and privacy assurance path for data communication by learning the node activity according to past and present actions and calculating the mean trust value periodically.

3. Node Activities Learning Approach

To build a secure and privacy path it is important to recognize the trusted nodes in the network. It can be identified through continuous monitoring of a node transition activity during a communication. In most cases, a node reacts to a request by assisting or denying to serve. The cause of denial of service is rightful because of the scarcity of the resources or congestion at the node, or because of the selfishness or by a malicious intrusion it occurs is a question

to solve. This proposal tries to learn the activities and implement an algorithm to predict it probable future action state based on it Mean Trust Value (MTV) to build a secure route in WIRELESS NETWORKS.

3.1 Node Activities Learning (NAL) Method

The NAL method learns the actions of a node to classify the node state into a defined type of class of actions. According to the past activity and actions of the node, we classify the node class into four different classes as, "*Trustable (T), Non-Trustable (NT), Selfish(S)* and *Malicious (M)*." To classify a node class, we learn the function of an intermediate node which generally supports in routing and also acknowledges the routing errors. Each intermediate node in a route initially considering in class *T*, but during the communication cycle, its state can be changed due to the following reasons as mentioned in Table-1.

Table 1. Activity State Class Change Reasons

Initial State	Learned State	Reasons for the State Changes	Prob. Of Class Possible
Trustable	Non-Trustable	Node serve as denial of service as not in communication range, congestion, frequent link failure.	Trustable Non-Trustable
Trustable	Selfish	If a node coordinate during the path construction process, during data routing it drops the packets due to resource scarcity is not reply to the controlling messages.	Trustable Non-Trustable Malicious
Trustable	Malicious	Node serves as a denial of service as not in communication range and identified as not forwarding packets, when the route is manipulating, unwanted message broadcasting or any other suspicious activity is observed.	Malicious

To learn the characteristic of the class state, we need to predict node class attributes accurately. The nature of wireless networks in real time can change unexpectedly at different points for different reasons. This changes the behavior of the node arbitrarily whenever in the real-time network. It can also be attributable to several attacks or lack of resource practice required to preserve network links and packet forwarding.

The action-based state estimation will be performed by utilizing a probabilistic characteristic association [28] to the properties of the class state reasons mention in Table-1. Here we considered the activities changes that are mostly due to the power level of the node where it rightfully rejects a request due to low power, in case of selfish or due to an attack it misinforms to conserve the power. Proper restructuring can re-establish the reliability of the selfish and malicious nodes. This restructuring is negative because of diminishing in energy sources. A malicious node can be a considered as an unsuccessful node, but if the malicious behavior is unbalanced, it is no longer measured trustworthy, and it has to the left alone. If the node activity fails, routing observed at regular intervals is stable, then the node can be faithful.

Even though there is no precise source for action transforms of a node we considered these common action changes occur in a various communication network. The learning method implements a probability of activity transformation prediction to understand the accurate further state class of a node.

Let's assume that a network having a set of trusted nodes as "*Z = {n1,n2,n3, ... }*", and according to the classified state change classes we have a vector *V* having the defined class and its probable attributes values represent as, "*V = {[T(a_1,a_2,a_3,...)], [NT(a_1,a_2,a_3,...)], [S(a_1,a_2,a_3,...)], [M(a_1,a_2,a_3,...)]}*". The intermediate nodes change their state arbitrarily or remain same during the communication in a particular time interval *Q* as shown in Figure 1.

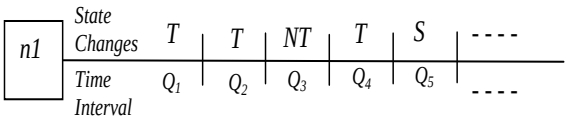

Figure 1. A node state change illustration with a time interval

So, the learned probability of the node activity transformation based on the change of state in an interval of time Q_i can be presented as,

$$P_{tform} = prob((_{pn+1} \rightarrow V_{n+1}) | (P_n \rightarrow V_n) \quad (1)$$

However, the dynamic action of the node can alter entirely in the surveillance time interval at once. For example, at a time interval, Q_i a node energy level is low, and its state is changed to selfish *S* to survive. So, to pretend the probable future action mean, A_{mean} of the collective state changes is computed to decide the probable action.

$$A_{mean} = \frac{\Sigma\, Individual\ States}{No.of\ Intervals} \quad (2)$$

Using Eq. (2) We find the mean value A_{mean} of each state class. The class which has the highest value of A_{mean} will be probable state of the node. This NA learning process can be utilized to illustrate a big extent of threats related to node malfunction and is associated with node action classification. This will make enormous the action of a node probability association to the present state of class in this time of communication. This prediction of expectations characterization models for the nodes action inference depend on supposition will be self-reliance for suggesting the probable state class of action. This NA learning is further utilized to compute the node MTV to create secure communication.

3.2 Secure and Privacy using NAL

According to the mean of action, value learned for a period the current state of the node is predicted. But to utilize it for the future routing and degree privacy, we will compute its MTV. All the nodes initially in the network considered trusted, and their MTV is assigned to 1. If a node *MTV=1* then it is considered highest trusted and *MTV=0* is the lowest.

To compute the MTV we consider two stage of node recognition class as, " Trusted stage, S_{tage}" or "Malicious stage, M_{stage}." In the case of T_{stage} a node is predicted as trusted and in case of M_{stage} it is predicted as malicious for the current period of the probability prediction.

To retain the level of trustiness a node, it has to maintain the throughput rate according to their MTV. If a node current "MTV=0.91" then it has to maintain its throughput rate in ~ 90% to retain its trustiness. In case of reduction, it is considered as $M_{stage,}$ and its new *MTV* is computed using Eq. (3), which is derived from the Bayesian formulation reputation system [29].

$$MTV\ (n) = \int_{q=0}^{Q} \frac{\sum T_{stage} + 1}{\sum T_{stage} + \sum M_{stage} + 2} \qquad (3)$$

The *MTV* of a node decides its current node beliefs for a period of the communication cycle. As the *MTV* of node varies with the period for the communication cycle, it is needed to compute a collective MTV as C_{MTV} after a defined period for avoidance in case of low trustiness. As a node have to undergo a different type of transformation state due to the dynamic environment of the network, so its *MTV* also changes accordingly. But, to remove a malicious node below the trust threshold, we calculate the C_{MTV} using Eq. (4) over period *p* time intervals.

$$C_{MTV} = \frac{\int_{i=0}^{p} \sum MTV(n)}{p} \qquad (4)$$

The value of C_{MTV} range between *0* and *1*. The minimum C_{MTV} threshold value is set to > *0.5* to retain in the network node else the node will be eliminated. This method of identifying the trusted node supports to build secure and privacy route for the communication and also provides the fairness to nodes to retain in-network for longer to regain their trustiness. The retaining of the routing nodes in the network supports in achieving network stability and throughput. In the following section, we evaluate this method to justify the improvisation in secure routing.

4. Experimental Evaluation

The evaluation of the NAL based security and privacy routing utilizing the trustiness is performed using the API of GMS simulator. This experiment undertakes to assess the hopeful actions changes of the intermediate node in relative to the number of packets transitions through them to the destination node being transmitted by the source node. The NAL methods are implemented over AODV routing protocol to evaluate the effectiveness.

4.1 Simulation Setup

To perform the simulation a wireless environment is configured, where nodes are randomly distributed in a terrain dimension area with others network parameters to support the communication. Data are transmitted in a constant bit rate from the source node to the destination node with a variation of *0 - 10m/s* mobility speed. The parameters configured for the simulation are listed in Table-2.

During the simulation, the action of a node changes according to the state of class configured. We considered the packet delivery, link failure and denial of service attributes to predict the probability mean trust over the AODV routing. To evaluate the outcome of the simulation, we analyze the comparison results of "*Throughput*," " *Packet Dropped*," "*Control Overhead*" and *"End-2-End Delay"*. To analyze the improvisation in the secure routing, we compare the NAL approach with "TMS-BF" [27], "FACE" [13] and "AODV" [30].

Table 2. Simulation Parameters

Configuration	Parameter Values
Simulation Time	1000s
Terrain Area	1000m X 1000m
No.of nodes	100
Mobility Model	RWP
Mobility	0 to 20m/s
Pause Time	30s
Packet Size	512 bytes
CBR Rate	4pkts/s
No.Of Malicious Nodes	5,10,20,30,40,50

4.2 Result Analysis

This section presents the analysis of the results obtained through a varying number of malicious nodes into the network from 5 to 50 numbers for a period 600 seconds simulation having 25 source-destination pairs.

- ***Throughput*:** Throughput measure the success rate of data packet delivered to the destination node. Figure 2 shows the throughput comparison between the approaches. All the approaches show above 90% of throughput in the presence of 10 number of the malicious nodes, but with an increasing number of malicious nodes >10 show dropping in throughput. In comparison to the existing approaches the NAL approach show 20% higher throughput. Accurate forecasting is possible with nodes that are supported and unsupported to support forecasting. Accurate predictions authorize nodes to remain in the network, helping to stabilize and sustain the improvisation in throughput.

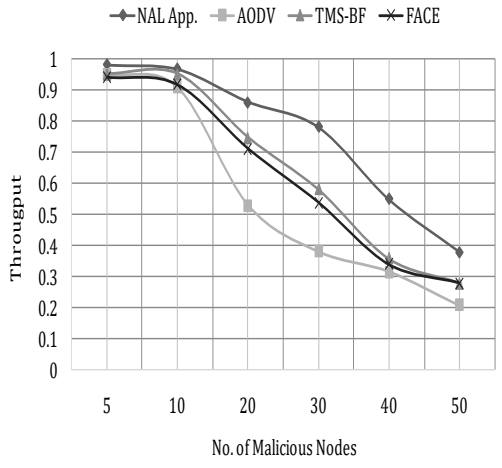

Figure 2. Throughput Comparison

- ***Control Overhead*:** The measure of the control overhead compute the network additional processing load in terms of the control message exchange for controlling the communication activities. Figure 3 showed the comparison of control overhead between the existing and proposed NAL approach. A difference of an average 15% less number of packet loss being observed compared to the existing approaches, it is due to the trusted and secure route communication. Even the availability of trusted node helps to retain a path for longer to communicate whereas another approaches lose their path due to the malicious activities.

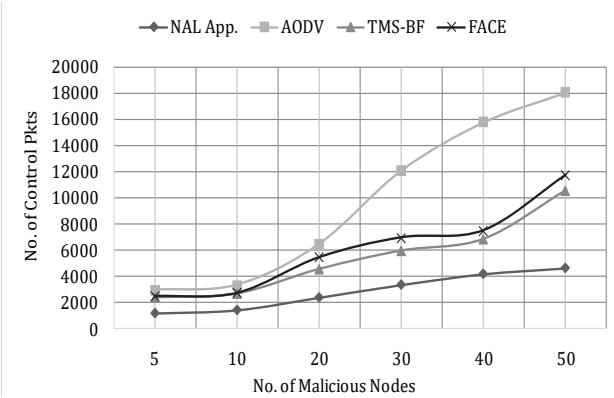

Figure 3. Routing Overhead Comparison

- ***Number of Packet Dropped*:** Packet loss in a network measure the number of denial of service by a node for the request packet transition. Figure 4 shows the comparison of packet dropped between the proposed NAL and existing approaches. It shows that with increasing number of malicious node all the approaches have a linear increase in loss packets. But the NAL approaches show the least among all due to constructing the trusted node route which supports to retain the path for long and smooth data routing to minimize the packet drops.

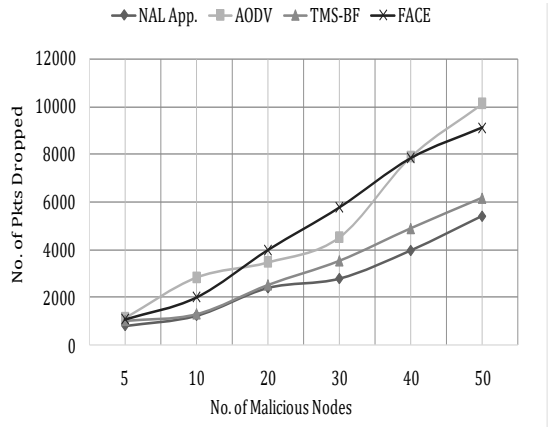

Figure 4. Packet drop Comparison

- ***End-to-End Delay*:** It measures the average time taken by a node for data packet delivery. Figure 5 shows the end-to-end delay comparison of the proposed NAL and existing approaches. It shows with increasing number of malicious nodes the delay between the ends delivery also increasing. They all show a nearby delay up to 20 number of malicious, but having >20 number of the malicious node the proposed shows 10ms less delay in comparison due to the secure path transmission and the trusted nodes can achieve 99% packet transmission, minimizing the total delay between source and destination nodes.

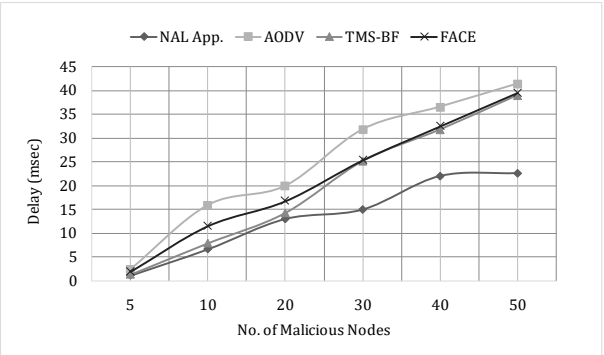

Figure 5. End-to-End Delay Comparison

5. Conclusion

This paper presented a Node Activities Learning approach based on the probability of activity transformation prediction and Mean Trust Value (MTV) to build a secure and privacy routing. The effect of a change in node activity on physical communication resolves the node isolation problem. Most previous approaches isolate nodes in the network depending on packet forwarding and request-response evaluations. This separation enlarges the network preservation overhead, resulting in further unsteadiness and low performance. The proposed NAL approach solves this problem by utilizing trust and malicious prediction and computing the MTV. It uses probabilistic models to calculate possible node trusts to minimize unfair node isolation. A node trust calculation based on possible node trust improves the node isolation frequency. Experimental results show a very high improvement of throughput with lowering the network overhead, packet loss, and end-to-end delay.

References

[1] M. S. Pathan, N. Zhu, J. He, Z. A. Zardari, M. Q. Memon, and M. I. Hussain, "An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs," *Future Internet*, Vol.10, No.16, 2018.

[2] M. Li, S. Salinas, P. Li, Ji. Sun, and X.Huang, "MAC-Layer Selfish Misbehaviour in IEEE 802.11 Ad Hoc Networks: Detection and Defence," *IEEE Trans. On Mobile Comp.*, Vol. 14, No. 6, June 2015.

[3] M. N. Ahmed, A.H. Abdullah, H. Chizari, and O. Kaiwartya, "Flooding Factor based Trust Management Framework for secure data transmission in MANETs," J. *King Saud Univ. Comput. Inf. Sci.*, Vol.29, pp.269-280, 2017.

[4] N. Marchang, R. Datta, and S. K. Das, "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks," *International Journal of IEEE Transactions on Vehicular Technology*, Vol. 66, No.2, pp.1684 - 1695, 2017.

[5] A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "A Survey on Trust-Based Detection and Isolation of Malicious Nodes In Ad-Hoc and Sensor Networks," *International Journal of Frontiers of Computer Science*, Vol.9, No.2, pp.280-296, 2015.

[6] A. Khana, M. Imranb, H. Abbasa, and M. Hanif Duradb, "A detection and prevention system against collaborative attacks in Mobile Ad hoc Networks," *Elsevier Future Generation Computer Systems*, Vol. 68, pp.416-427, 2016.

[7] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust-Distortion Resistant Trust Management Frameworks on Mobile Ad Hoc Networks: A Survey," International *Journal of IEEE Communications Surveys & Tutorials*, Vol.18, No.2, pp. 1287 - 1309, 2016.

[8] T. Shu, and M. Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks," *International Journal of IEEE Trans. On Mobile Comp.*, Vol. 14, No. 4, April 2015.

[9] R. Hinge, and J. Dubey, "Opinion based trusted AODV routing protocol for MANET," *In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS), ACM*, NY, USA, 2016.

[10] K. Paul and D. Westhoff, "Context-aware detection of selfish nodes in DSR based ad-hoc networks," *in Proc. IEEE Global Telecommunication. Conf.*, Vol. 1, pp. 178-182, 2002.

[11] J.-H.Cho, I.-R. Chen, and S. J. Kevin, "Trust threshold based public key management in mobile ad hoc networks," *Elsevier Ad Hoc Networking*, Vol. 44, pp. 58-75, 2016.

[12] K. Ullah, R. Das, P. Das, and A. Roy, "Trusted and secured routing in MANET: An improved approach," *International Journal of IEEE Symposium on Advanced Com. and Comm.*, pp. 297 - 302, 2015.

[13] S. K. Dhurandher, M S. Obaidat, K Verma, P Gupta, and P Dhurandher, "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems," *IEEE Systems Journal*, Vol. 5, No. 2, 2011.

[14] Z. Wei, H. Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning," *IEEE Transactions on Vehicular Technology*, Vol. 63, No. 9, November 2014.

[15] T. Jenitha, and P. Jayashree, "Distributed Trust Node Selection for Secure Group Communication in MANET," *In Proc. of International Conf. on IEEE 4th Advances in Computing and Communications*, 2014.

[16] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks," *International Journal of Wireless personal communications*, Vol. 69, No. 2, pp. 805-826, 2013.

[17] H. Xia, Z. Jia, L. Ju, X. Li, and Y. Zhu, "A subjective trust management model with multiple decision factors for MANET based on AHP and fuzzy logic rules," *in Proc. IEEE/ACM Green Computer Communication*, 2011.

[18] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, "Trust management systems for wireless sensor networks: Best practices," *International Journal of Computer. Communication*, Vol. 33, No. 9, pp.1086-1093, 2010.

[19] Z. Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning," *IEEE Transactions On Vehicular Technology*, Vol. 63, No. 9, November 2014.

[20] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Networks," *Proc. ACM MobiCom '00*, pp. 255-265, 2000.

[21] G. Zhan, W. Shi, and J. Deng, "Design and implementation of tarf: A trust-aware routing framework for WSNs," *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No.2, pp.184-197, 2012.

[22] T. Zia, "Reputation-based trust management in wireless sensor networks," *In Proc. International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, pp.163-166, December 15-18, 2008.

[23] Q. He, D. Wu, and P. Khosla, "SORI: A s1ecure and objective reputation-based incentive scheme for ad-hoc networks," *in Proc. IEEE Wireless Communication. Network. Conf*, Vol. 2, pp. 825-830, 2004.

[24] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, "Trust management systems for wireless sensor networks: Best practices," *Computer Communication*, Vol. 33, No. 9, pp. 1086-1093, 2010.

[25] X. Mao, and J. McNair, "Effect of on/off misbehavior on overhearing based cooperation scheme for MANET," *in Proc. Military Communication. Conf*, pp. 1086-109, 2010.

[26] R. Venkataraman, M. Pushpalatha, and T. Rama Rao, "Regression-based trust model for mobile ad hoc networks," *International Journal of IET Information Security*, Vol. 6, No.3, pp.131 - 140, Sept. 2012.

[27] C. E. Xi, S. Liang, M. A. JianFeng, and M. A. Zhuo, "A Trust Management Scheme Based on Behaviour Feedback for Opportunistic Networks," *Network Technology and App. in China Comm*, April 2015.

[28] M. Deno, and T. Sun, "Probabilistic trust management in pervasive computing," *In Proc. International Conference on Embedded and Ubiquitous Computing*, Vol. 2, pp. 610-615, 2008.

[29] A. Josang and R. Ismail, "The beta reputation system," *in Proc. 15th Bled Electron. Commerce Conference*, pp. 41-55, 2002.

[30] A. Perkins, E. Belding-Royer, and S. Das, "Ad-hoc On-Demand Distance Vector (AODV) routing," *Mobile Ad hoc Networking Working Group Internet draft*, Vol. 5, No. 2, pp. 32-34, July 2003.