Communications and Network, 2013, 5, 185-191
http://dx.doi.org/10.4236/cn.2013.53021 Published Online August 2013 (http://www.scirp.org/journal/cn)

Classification of Selfish and Regular Nodes Based on Reputation Values in MANET Using Adaptive Decision Boundary

Amir Khusru Akhtar[1], **G. Sahoo**[2]
[1]Department of Computer Science and Engineering, Cambridge Institute of Technology, Ranchi, India
[2]Department of Information Technology, Birla Institute of Technology, Mesra, Ranchi, India
Email: akru2008@gmail.com, gsahoo@bitmesra.ac.in

Received May 1, 2013; revised June 10, 2013; accepted July 10, 2013

ABSTRACT

A MANET is a cooperative network in which each node has dual responsibilities of forwarding and routing thus node strength is a major factor because a lesser number of nodes reduces network performance. The existing reputation based methods have limitation due to their stricter punishment strategy because they isolate nodes from network participation having lesser reputation value and thus reduce the total strength of nodes in a network. In this paper we have proposed a mathematical model for the classification of nodes in MANETs using adaptive decision boundary. This model classifies nodes in two classes: selfish and regular node as well as it assigns the grade to individual nodes. The grade is computed by counting how many passes are required to classify a node and it is used to define the punishment strategy as well as enhances the reputation definition of traditional reputation based mechanisms. Our work provides the extent of noncooperation that a network can allow depending on the current strength of nodes for the given scenario and thus includes selfish nodes in network participation with warning messages. We have taken a leader node for reputation calculation and classification which saves energy of other nodes as energy is a major challenge of MANET. The leader node finally sends the warning message to low grade nodes and broadcasts the classification list in the MANET that is considered in the routing activity.

Keywords: MANETs; Regular Node; Selfish Node; Adaptive Decision Boundary; Feature Value; Noncooperation

1. Introduction

Ad hoc wireless networks utilize multi-hop radio relaying and operate without support of any fixed infrastructure. This makes the routing complex compared to other networks. Nodes must communicate to each other regarding information about other nodes. A node can transmit and receive data, as well as act as a router for routing packets for other nodes. A node forwards packet in an ad hoc network using the routing algorithms presented in [1-7]. Attacks are a challenge for the ad hoc routing protocols. Some of the attacks are modification, fabrication, wormhole attack (tunneling), blackhole attack, denial of service attack, invisible node attack, sybil attack, rushing attack and non-cooperation. To short out these attacks some secured routing protocols are developed these are Ariadne [1], ARAN (Authenticated Routing for Ad hoc Networks) [2,3], SEAD (Secure Efficient Ad hoc Distance vector routing) [4], SRP (Secure Routing Protocol) [5] etc. Most of the attacks based on manipulations of routing data can be detected by the use of a secure routing protocol like Ariadne, ARAN, and others [6,7]. However these secure routing protocols fail when nodes drop packets of other nodes, as they concentrate only on the detection or modifications of routing data but noncooperation (selfishness) is still in its natal stage. To deal with selfishness we have so many solutions in reputation based model such as Watchdog and Pathrater [8], CONFIDANT [9,10], CORE [11], OCEAN [12] and others [13-18]. These solutions [8-18] reduce selfishness but a cooperative network is still affected because these models have a stricter isolation policy. In a cooperative network if nodes are isolated from routing and forwarding using lesser reputation value then it will damage the entire network or cause network failure. In this paper we have proposed a mathematical model using an adaptive decision boundary which classifies nodes in two classes: (selfish and regular nodes) as well as it assigns the grade to individual nodes. The grade is computed by counting how much passes the algorithm takes to classify a node and it is used to define the punishment strategy as well as enhance the reputation definition of traditional reputation based mechanisms [8-18]. This paper is organized as follows. Section 2 describers the background and related work. Section 3 presents the mathematical model for the classification of nodes in MANET. Section 4 gives the experimental analysis in which we have used indigenous tool written in "C" language for classification of node, grade assignment and punishment definition. We verified it with different experimentations. Section 5 concludes the paper.

2. Background and Related Work

Mobile wireless network, capable of autonomous operation operates without base station or infrastructure. In this network nodes cooperate with each other to provide connectivity and operate without centralized administration. But when nodes drop packets of others due to honest or malicious causes they are called selfish nodes [19]. A node is called selfish if it drops packets of others due to either honest causes such as collisions, channel errors, or buffer overflows or maliciously such as to save its energy or bandwidth, blackhole or wormhole attack, network congestion. A selfish Node degrades efficiency of packet transfer and accelerates the packet delivery time and packet loss rate and finally creates Network Partitioning. To enforce cooperation and to minimize battery usage Md. Amir Khusru AKhtar and G. Sahoo [20] proposed a novel methodology for securing adhoc network using friendly group model in which they used two NIC cards to partition a MANET into many friendly groups/ subnets. This model enforces cooperation because it minimizes battery usage which is the genuine cause of selfishness but this model is not suitable for all applications.

For the intrusion detection in MANET a classification algorithms was proposed [21], it is an innovative approach but not validated with real world data. We have other methods [22,23] for the detection of selfish node but these proposed algorithms consumes more energy. Paper [24] defines a secure routing protocol with node selfishness resistance in MANETs but this protocol still consumes more energy.

We have lots of methods to detect selfish nodes that are categorized into incentive-based methods and reputation-based methods. The first mechanism discourages a node to become selfish by giving virtual money/credits when a node forward packets of others. These credits are required when a node want to send or receive its own packets. Another method [17] proposed by Buttayan and Hubaux uses virtual currency, called nuglets to detect a selfish node. In this method a nuglet counter is incremented monotonically when it forwards a packet for others. When a node wishes to send its own packet, then enough credits are required as the system checks for a certain threshold value otherwise it is not allowed to send packets. The limitation of this method is that it requires tamper proof hardware to maintain the nuglet.

On the other hand, the reputation-based methods detect a selfish node and take appropriate action by means of reputation system that detect and defines the rate a selfish node. In these mechanisms reputation is defined on the basis of participation seen by others [16]. The good reputation indicates honest participation in the network activity otherwise it is marked as selfish.

Since we are classifying a MANET on the basis of reputation values that is why we are focusing on "Reputation Based Mechanisms". A survey of trust and reputation management systems in wireless communications [25] shows the current status of reputation based systems and its limitation in terms of energy usage and noncooperation.

The first method on detection of routing misbehavior was proposed by Marti *et al.* called the Watchdog and Pathrater [8]. It is to be used over the DSR [6] routing protocol to alleviate selfish and malicious routing misbehavior in MANET. Watchdog module is responsible for neighbor monitoring and identifying malicious and selfish nodes whereas Pathrater module evaluates the overall reputation of nodes and defines route by excluding the selfish or misbehaving nodes. In this mechanism a selfish node is rewarded instead of any punishment for the misbehavior.

The CONFIDANT protocol proposed by Buchegger *et al.* [9,10], in which the first module called Monitor that is responsible for observing and recording the misbehavior of neighboring nodes. The second module the reputation system is responsible for calculating the reputation of nodes on the strength of direct observation and indirect observation. The third module trust manager is collects warning messages from friends, and finally the fourth module the path manager defines the path for routing by excluding selfish nodes. In this protocol, each node monitors its neighborhood behavior and observed misbehavior is reported to the reputation system. If the misbehavior is not tolerable then it is reported to the path manager, and then the path manager excludes the nodes from the routing path and calculates new paths. This method has weaknesses due to inconsistent evaluation problem, for the reason that every node has different evaluations for the same node and has difficulty to identify correct selfish node. Another limitation is in terms of more battery power consumption for a node located in the center of network in comparison to situated at the periphery of the network.

The CORE protocol [11] proposed by Michiardi *et al.*, uses three reputations (subjective, indirect and functional). This mechanism uses reputation table to maintain the reputation value for each node and the watchdog mechanism to observe that a requisite function is performed by the requested node or not. The reputation is defined on direct observation and on the basis of information provided by others nodes. The reputation value will facilitate a node to decide the selfishness of a requesting node and finally guide whether to serve or to decline the request.

A lot of research work [12-18] shows the usage of reputation value in the detection and exclusion of selfish node from a mobile adhoc network. All these methods have limitation due to its stricter punishment strategy because they isolate the nodes from routing activity on the basis of lower reputation value and thus reduce the overall strength of nodes in the network. Since a cooperative network is based on the nodes strength and thus the network does not perform better.

3. Proposed Work

3.1. Adaptive Decision Boundary

In this paper, we are showing a classification model based on Adaptive Decision Boundary [26] that classifies a network into selfish and regular nodes as well as it assigns grade to individual nodes. The grade is computed by counting how many passes are required to classify a node and it is used to define the punishment strategy as well as enhances the reputation definition of traditional reputation based mechanisms [8-18]. The punishment strategy is defined in section 3.5. This model works fine with the existing routing protocols and solutions. We have assumed a leader node in our work which is responsible for defining an adaptive decision boundary explained in section 4.1.

In this work an adhoc network is classified into two classes selfish and regular. The classification of nodes reputation values modeled mathematically using Adaptive Decision Boundary [26]. We have defined a linear decision boundary to classify nodes reputation values into two classes in which a network has M features. Feature values are taken from reputation values and the discriminant function is of the form

$$D = w_0 + w_1 x_1 \cdots + w_M x_M \tag{1}$$

The adaptive decision boundary D = 0 is the equation of the decision boundary and lying between the two classes (selfish and regular). The weights are w_0, w_1, …, w_M are selected for better analysis of the network. Through this we classify a MANET with reputation values called feature values obtained from literature [9-16, 19,25]. A network with M feature values $X = (X_1, X_2, \ldots, X_M)$ is classified in to two classes: regular class with reputation value 1 (if $D \geq 0$) and selfish class-1 (if $D < 0$). **Figure 1** shows the two classes (selfish and regular denoted as S and R respectively) which are separated by a straight line.

3.2. Problem Definition and Proposed Solution

In this paper we are classifying the selfish and regular nodes on the basis of reputation values in a MANET using adaptive decision boundary. The existing methods [8-18] have limitation due to its stricter punishment strategy because they isolate nodes from network participation having lesser reputation value and thus reduce the total strength of nodes in a network. The lesser number of nodes reduces network performance, degrades efficiency of packet transfer, accelerates the packet delivery time, enhances packet loss rate and creates Network Partitioning. That is why we have proposed this classification technique. The proposed solution to tackle this problem is described using the following steps

Step 1: Initially we have obtained the reputation values of all nodes in a network using existing reputation system as defined in [8-12].

Steps 2: After that true class or desired value of a node is defined as defined in section 3.3.

Steps 3: Then nodes are classified into selfish and regular classes based on reputation values by using the algorithm 3.4. Further, the number of passes is used to define grade.

Step 4: Finally punishment criteria are defined on the basis of grade. For example we have included medium grade (G_{MED}) selfish nodes in network participation with proper warning messages and low (G_{LOW}) grade nodes are excluded form network participation. The punishment criterion is defined in section 3.5.

3.3. Defining True Class or Desired Value

In this model we are assuming the true class or desired value (d) by +1 and by −1. A +1 value indicates a regu-

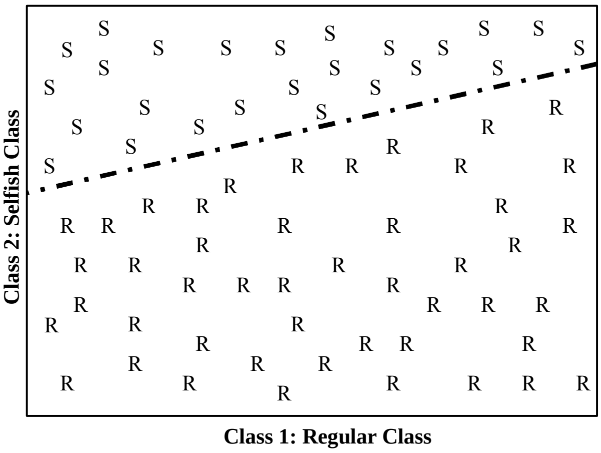


Figure 1. Nodes reputation values are linearly separable.

lar class and −1 denotes a selfish class. The true class of a node is defined on the basis of minimum number of passes to classify in true classes +1 or −1 on the basis of nodes reputation value shown in **Figure 2**.

For example, on the basis of reputation value a node of a MANET takes 20 passes to classify in selfish class and 30 passes for regular class. The selfish class takes minimum number of passes to classify, so in this example the node is classified in selfish class and d = −1.

The classification, true class definition and grade calculation is performed by executing adaptive_decision_boundary() function. This function counts how many passes are required to match the value of d with Discriminant "D" and it finds the true class on the basis of minimum number of passes. Then the grade is defined using **Table 1** and it is used to define the punishment criteria explained in section 3.5.

3.4. "C" Language Function for the Classification of Nodes in a MANET Using Single Numeric Feature

In this section we are presenting the adaptive decision boundary algorithm to classify selfish and regular nodes based on reputation values in MANET.

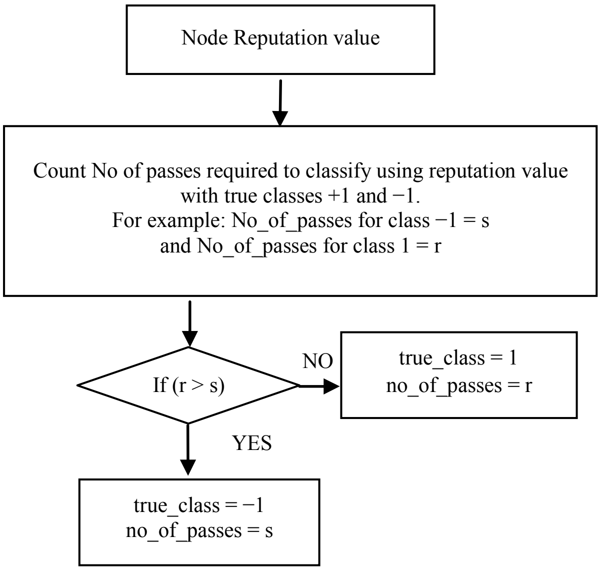

Node Reputation value
Count No of passes required to classify using reputation value with true classes +1 and −1.
For example: No_of_passes for class −1 = s
and No_of_passes for class 1 = r
If (r > s)
NO
true_class = 1
no_of_passes = r
YES
true_class = −1
no_of_passes = s

Figure 2. Flowchart showing nodes true class calculation.

Table 1. Grade assignment and punishment crieteria.

Number of passes required to classify	Grade	Punishment criteria
Less than or equal to 10	G_{HIGH}	No
Less than or equal to 30	G_{MED}	Warning message
Greater than 30	G_{LOW}	Exclude nodes from routing activity

```
/* Classification using Adaptive decision boundary */
    adaptive_decision_boundary() {
    do{
        for(i=1;i<=2;i++){
            if(i%2==1)
            {++s; j=0;}
        else
            {++r; j=1;}
            d=a[j][2];
            x=a[j][1];
            D=w0+w1*x;
            if(D>=0) D=1;
            else  D=-1;
            if(D!=d){
                ++r;
                w0=w0+c*d*k;
                w1=w1+c*d*x;}
                if(r>s)
                    {tc=-1; pass=s;}
                else
                    { tc=1; pass=r;}
            }
}while(D!=d);
    if(pass <= 10)
        strcpy(grade,"High");
    else if(pass <= 30)
        strcpy(grade,"Medium");
    else if(pass > 30)
        strcpy(grade,"Low"); }
```

3.5. Grade Calculation and Punishment Criteria

Grade is calculated by counting how many passes the algorithm takes to classify. **Table 1** shows the number of passes, grade of a node and punishment criteria.
where,

G_{HIGH}: High grade
G_{MED}: Medium grade
G_{LOW}: Low grade

4. Experimental Analysis

4.1. Experimental Assumption

The experimental analysis is based on section 3. To find an adaptive decision boundary to classify nodes of a MANET reputation values are taken into consideration. We have taken a network of sixteen nodes with one leader node as given in **Figure 3**.

The leader node is an intelligent node of the adhoc network, which has good knowledge of the network and having high computation capability to process and maintain the history of the transaction and responsible for calculation of reputation value in the network. A leader node could be a captain's laptop in a battle zone. The leader node calculates the adaptive decision boundary to classify a network from the gathered reputation values [8-18] of nodes in the network and then assign grades. On that basis of grade punishment criterion is defined as given in **Table 1**.

The leader node maintains the reputation table as defined in **Table 2**. We have taken node identification number (ID), x denotes one dimensional feature or reputation value and d is the true class or desired value for a node obtained using the code defined in section 3.4.

4.2. Result and Discussion

We have classified nodes into two classes selfish and regular using the solution defined in section 3.2 into two classes using the following parameters.

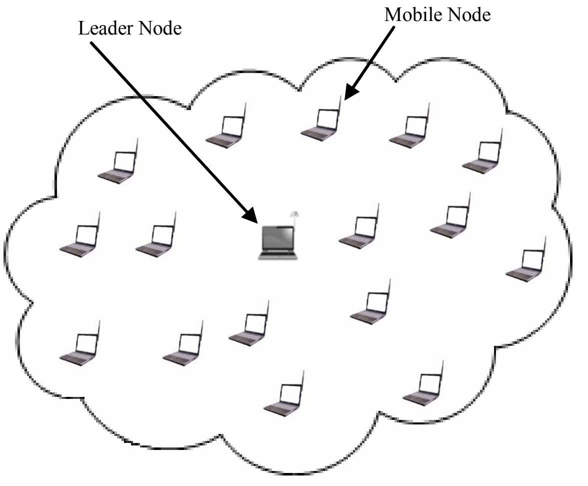


Figure 3. A MANET of sixteen nodes with a leader node.

Table 2. MANET reputation table.

ID	x	d
1	−5	−1
2	−1	1
3	−6	−1
4	1	1
5	0	1
6	−3	−1
7	−1	−1
8	2	1
9	−4	−1
10	2	1
11	3	1
12	4	1
13	5	1
14	1	1
15	−5	−1
16	−3	−1

d: true class or desired value defined in section 3.3.

D: discriminant function defined in section 3.1.

w_0 and w_1: small random values used to speedup the classification.

c: a positive constant that controls the step size for reputation adjustment needed for classification.

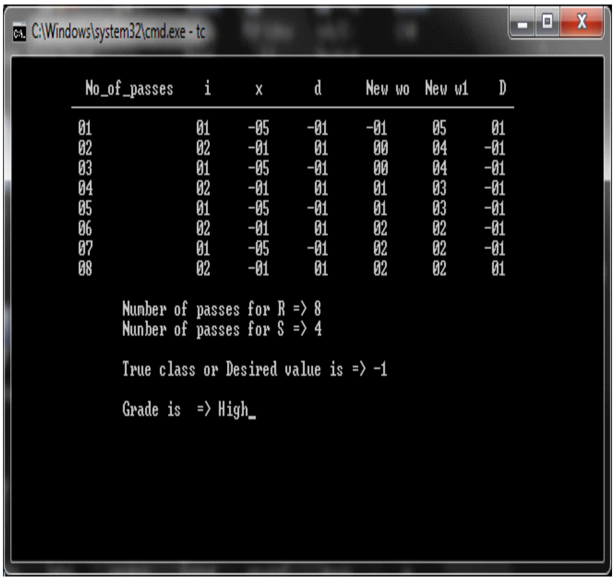
k: a positive constant denoting average absolute reputation value in the problem required to minimize the number of passes.

Choosing the correct c and k values will minimize number of passes to classify as defined in [26].

Figure 4 shows the output generated using code given in section 3.4 by processing **Table 2**. The constant c and k both chosen to be 1. Initially the weights for w_0 and w_1 are initialized with 0. The output shows the classification of first two nodes with attributes No_of_passes, I denote node number, x is the reputation value, d the true class, new w_0 and w_1 the small random values and the discriminant D. We have also shown how many passes are required to classify a node into regular or selfish classes and the equivalent grade. Further, grade is used to define the punishment criteria as given in **Table 1**.

5. Conclusion

This paper has seen MANETs in the noncooperative



```
   No_of_passes    i      x       d       New wo  New w1    D
  ____________________________________________________________

  01               01    -05     -01     -01      05       01
  02               02    -01      01      00      04      -01
  03               01    -05     -01      00      04      -01
  04               02    -01      01      01      03      -01
  05               01    -05     -01      01      03      -01
  06               02    -01      01      02      02      -01
  07               01    -05     -01      02      02      -01
  08               02    -01      01      02      02       01

         Number of passes for R => 8
         Nunber of passes for S => 4

         True class or Desired value is => -1

         Grade is  => High_
```

Figure 4. Output generated using code given in section 3.4.

environment. It has defined how mathematical model has been used to classify selfish nodes in MANETs. We have introduced a mathematical model showing the classification of nodes (regular and selfish classes) in MANETs. This model is verified by experimentation and gives acceptable accuracy and provides a solution for secured routing also when a network having poor strength of nodes. The major problem with MANET is the node strength because existing solutions have a stricter punishment policy and they isolate the nodes having lesser reputation value and thus reduces the total strength of nodes in a network. Because a cooperative network is based on node strength and thus the network does not perform better. So, this model gives a more accurate classification and provides the extent of noncooperation that a network can allow depending on the current strength of nodes for the given scenario. Thus our model includes medium grade (G_{MED}) selfish nodes in network participation with proper warning messages and excludes only the low (G_{LOW}) grade nodes.

6. Acknowledgements

The authors are thankful to anonymous referees for their valuable comments and suggestions to improve the quality of the paper.

REFERENCES

[1] Y. Hu, A. Perrig and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Proceedings of the* 8*th Annual International Conference on Mobile Computing and Networking*, September 2002, pp. 12-23. doi:10.1145/570645.570648

[2] K. Sanzgiri, B. Dahill, B. Levine, C. Shields and E. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," *The* 10*th IEEE International Conference on Network Protocols* (*ICNP*), 12-15 November 2002, pp. 78-87.

[3] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields and E. M. Belding- Royer, "Authenticate Routing for Ad Hoc Networks," *IEEE Journal on Selected Area in Communications*, Vol. 23, 2005.

[4] Y. Hu, D. Johnson and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks," *The* 4*th IEEE Workshop on Mobile Computing Systems and Applications*, June 2002, pp. 3-13.

[5] P. Papadimitratos, Z. Haas and P. Samar, "The Secure Routing Protocol (SRP) for Ad Hoc Networks," 2002.

[6] D. Johnson, D. Maltz, and Y.-C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," *IEEE Internet Draft*, April 2003.

[7] C. E. Perkins and E. Royer, "Ad-Hoc On-Demand Distance Vector Routing," *Proceedings of* 2*nd IEEE Workshop on Mobile Computing Systems and Applications*, 1999, pp. 90-100. doi:10.1109/MCSA.1999.749281

[8] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proceedings of the* 6*th Annual International Conference on Mobile Computing and Networking* (*ACM MobiCom* 2000), New York, 2000, pp. 255-265.

[9] S. Buchegger and J. Y. Le-Boudec, "Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks," *Proceedings of the* 10*th Euromicro Workshop on Parallel*, *Distributed and Network-Based Processing*, Canary Islands, 2002, pp. 403-410.

[10] S. Buchegger and J. Y. Le-Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness in Dynamic Ad-Hoc Networks," *Proceedings of MobiHOC*'02, June 2002, pp. 226-236.

[11] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Cooperation in Mobile Ad-Hoc Networks," In: J.-B., Borka and K. Tomaz, Eds., *Advanced Communications and Multimedia Security*, Kluwer Academic Publishers, 2002.

[12] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad Hoc Networks," Technical Report, Stanford Univ., Standford, 2003.

[13] R. Akbani and T. Korkmaz, "Enhancing Role-Based Trust Management with a Reputation System for MANETs," *URASIP Journal on Wireless Communications and Networking* 2011, 2011, p. 90.

[14] F. Wang. F. R. Wang, B. X. Huang and L. T. Yang, "COSR: A Reputation-Based Secure Route Protocol in MANET," *EURASIP Journal on Wireless Communications and Networking—Special Issue on Multimedia Communications over Next Generation Wireless Networks Archive*, Vol. 2010, 2010, pp. 1-11.

[15] S. R. Zakhary and M. Radenkovic, "Reputation Based Security Protocol for MANETs in Highly Mobile Disconnection-Prone Environments," *International Conference on Wireless On-demand Network Systems and Services* (*WONS*), 2010, pp. 161-167.

[16] S. Buchegger and J.-Y. L. Boudec, "Self-Policing Mobile Ad Hoc Networks by Reputation Systems," *IEEE Communications Magazine*, Ser. 7, Vol. 43, 2005, pp. 101-107. doi:10.1109/MCOM.2005.1470831

[17] L. Buttyan and J. P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," *Mobile Networks and Applications*, Vol. 8, No. 5, 2003, pp. 579-592. doi:10.1023/A:1025146013151

[18] A. Balasubramanian, J. Ghosh and X. Wang, "A Reputation Based Scheme for Stimulating Cooperation in MANETs," *Proceedings of the 19th International Teletraffic Congress*, Beijing, August 2005.

[19] T. Anusas-Amornkul, "On Detection Mechanisms and Their Performance for Packet Dropping Attack in Ad Hoc Networks," University of Pittsburgh, Pittsburgh, 2008.

[20] M. A. K. Akhtar and G. Sahoo, "A Novel Methodology for Securing Adhoc Network by Friendly Group Model," *The 4th International Conference on Networks & Communications* (*NetCoM*), Chennai, September 2012.

[21] A. Mitrokotsa and C. Dimitrakakis, "Intrusion Detection in MANET Using Classification Algorithms: The Effects of Cost and Model Selection," Ad Hoc Networks, Vol. 11, No. 1, 2013, pp. 226-237. doi:10.1016/j.adhoc.2012.05.006

[22] E. Hernández-Orallo, M. D. Serrat, J.-C. Cano, C. M. T. Calafate, and P. Manzoni, "Improving Selfish Node Detection in Manets Using a Collaborative Watchdog," *IEEE Communications Letters*, Vol. 16, No. 5, 2012, pp. 642-645. doi:10.1109/LCOMM.2012.030912.112482

[23] E. Hernández-Orallo, M. D. S. Olmos, J.-C. Cano, C. T. Calafate and P. Manzoni, "Evaluation of Collaborative Selfish Node Detection in MANETS and DTNs," *MSWiM'12 Proceedings of the 15th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2012, pp. 159-166.

[24] C.-T. Li, C.-C. Yang and M.-S. Hwang, "A Secure Routing Protocol with Node Selfishness Resistance in MANETs," *International Journal of Mobile Communications*, Vol. 10, No. 1, 2012, pp. 103-118. doi:10.1504/IJMC.2012.044525

[25] H. Yu, Z. Q. Shen, C. Y. Miao, C. Leung and D. Niyato. "A Survey of Trust and Reputation Management Systems in Wireless Communications," *Proceedings of the IEEE*, Vol. 98, No. 10, 2010, pp. 1755-1772. doi:10.1109/JPROC.2010.2059690

[26] E. Gose, R. Johnsonbaugh and S. Jost, "Pattern Recognition and Image Analysis," Prentice Hall of India Private Ltd., New Delhi, 2006.