JOURNAL OF PURE AND APPLIED MICROBIOLOGY, Aug. 2015. Vol. **9**, p. 161-168
SPECIAL ISSUE ON RECENT RESEARCH CHALLENGES IN BIO-MEDICAL APPLICATIONS

FGT2- ABR: Fuzzy Game Theory Trust Associativity Based Routing to Mitigate Network Attacks in Pervasive Health Monitoring Systems

K. Geetha[1] and P. Thangaraj[2]

[1]Department of Information and Technology, Excel Engineering College,
Nammakal, Tamilnadu, India.
[2]Department of Computer Science and Engineering, Bannari Amman Institute of Technology,
Sathyamangalam, Tamilnadu, India.

(Received: 15 March 2015; accepted: 11 May 2015)

With availability of hand held devices increasingly across various sections of the society the logical step in health care management is providing support anywhere and anytime. In scenarios like disasters where infrastructure may not be available for communication, intra communication between the devices without infrastructure is the logical design of networks where in communication is established between mobile devices. . A Mobile Adhoc Networks (MANET) is a group of mobile nodes communicating with each other without infrastructure or centralized administration. Security plays a very important role in such networks where personal data may be exchanged. Routing protocols should be able to cope with malicious nodes that disrupt correct routing protocol functioning by modifying routing information and other activities. In this paper, an enhanced Associativity Based Routing (ABR), Fuzzy Game Theory Trust ABR (FGT2- ABR), is proposed to mitigate network attacks with emphasis on pervasive health monitoring systems. The proposed method selects a route based on fuzzy game theory. Hello messages contain "AN - Avoid node" field based on malicious node detection. Membership functions used are successful deliveries number, Memory utilization and computed trust. Trust includes neighborhood trust based and recommendation based trust.

Key words: Mobile Adhoc Networks (MANET), Associativity Based Routing (ABR), Fuzzy game theory, Computed Trust.

Telecommunication technologies in healthcare has been successfully deployed for telemedicine applications leading to better accessibility of experts to patients in remote areas. Telemedicine has vastly improved the quality of healthcare due to its successful deployment. With emergence of mobile devices there is an urgent need to build frameworks for utilizing the mobile devices especially during disasters where healthcare management is critical. An option is to integrate telecare with Mobile Adhoc Networks (MANET). MANET characteristic is its dynamic nature with network topology frequently changing due to nodes unpredictable mobility[1]. Further each MANET mobile node has a router role when transmitting data over network. Networking functions for nodes in a MANET include routing and packet forwarding through a self-organizing and cooperative manner. The cooperative nature of nodes make securing the network challenging. To ensure security a MANET can be evaluated by[2]:

i. Availability: Which indicates that nodes are accessible by other authorized nodes at correct times.

ii. Confidentiality: Ensures that node related assets are accessed by authorized nodes only.

iii. Integrity: Ensures thatassets are modified only by authorized nodes and in an authorized way.

* To whom all correspondence should be addressed.
E-mail: srirajgeetha@gmail.com

iv. Authentication: Assures that participants in communication are authenticated.

v. Authorization: This assigns different access rights to different users / nodes.

vi. Resilience to attacks: Required to sustain network functionalities when few nodes are compromised.

vii. Freshness: Ensures malicious nodes do not resend packets captured earlier.

Conventional networks rely on distance-vector or link-state algorithms, based on periodic broadcast advertisements of all routers to update routing tables[3]. MANETs also use these algorithms, to ensure that route to all hosts are known. Many routing protocols have been proposed for MANETs to achieve efficient routing[4]. These are classified into three main categories: table-driven (or proactive) routing protocols, source-initiated (reactive or demand-driven) routing protocols and hybrid routing protocols. In table-driven routing protocols, every mobile node ensures consistent routing information in a network with updates.

Source-initiated on-demand (reactive protocols) protocols create routes only when needed by a source node. When a node wants a destination route it initiates a route request. Once a route is fixed, it is maintained by route maintenance procedure unless a route is inaccessible[5].

Route request packet is sent to all nodes in a network in ABR. In other words, search space determining route to destination node is equal to network space, and routing related traffic may waste bandwidth. The Associativity rule states that a Mobile Hosts (MH) association with neighbor changes when it migrates and its transiting period is identified by associativity 'ticks'. Associativity threshold[6] to distinguish association stability and instability is a beaconing interval function, mobile host's migration speed and wireless cell size. ABR compromises broadcast and point-to-point routing[7] and only maintains routes for sources that desire routes. Also, routing decisions are performed at destination with only the best route being selected and used while other routes are passive. This avoids packet duplicates and also the selected route tends to have more life due to associativity described.

Secure routing protocols cope with malicious nodes that disrupt correct routing protocol functioning by modifying routing information, fabricating false routing information and impersonating nodes[8]. Active attacks are actions like replication, modification and deletion of exchanged data. Some active attacks are easy against adhoc networks. These attacks are grouped as Impersonation, Denial of service, and Disclosure attack.

This work extensively focuses on security aspect ofMANET. This workuses fuzzymembership functions based on successful deliveries, Memory utilization and computed trust to find optimal secure route using game theory. Two Trust parameters neighbourhood based trust and recommendation based trust are defined in this work. Section 2 includes related early works in literature, Section 3 discusses methodology. Section 4 explains experimental results and finally section 5 concludes the paper.

Related work

A long lived routing method based on associativity for real time applications was proposed by Preveze and Safak[9]. The proposed work aimed to improve ABR algorithm to reduce nodes outage and decrease reconstructions needed to keep nodes in communication. ABR performance was compared to other long-lived relay selection algorithms in real-time applications and showed to have better performance.

Adding Quality of Services (QoS) extensions to ABR was tried out by Murad, et al.,[10]. Total operations performed and total messages exchanged remained same regarding operation and communication complexities analysis. There was an additional case where QoS-Route was invoked, specifically when an intermediate node failed to provide required QoS, when the source would be notified by a QoS-LOST message from that node and a new QoS-Route discovery initiated by source node.

An on-demand associativity-based multipath source routing protocol for MANETs to establish relatively stable path(s) between a communicating end nodes was proposed by Heo and Song[11]. A new notion to gauge nodes' temporal and spatial stability and paths interconnecting them was also attempted. The discovered paths were easier to maintain and suited QoS provisioning. The protocol reduced end-to-end delays leading to improved QoS provisioning and data communication performance. The new mechanism showed better QOScompared to DSDV, AODV and AOMDV.

Two innovative ABR methods called Associativity Tick Averaged ABR (ATAABR) and Alternative Enhancement for Enhanced Associativity Based Routing (AEABR) which were modifications of ABR were proposed by Preveze and Safak[12]. The new algorithms provided better life, link speeds and outage time results than Enhanced Associativity Based Routing (EABR). EABR performance was better than other relay selection algorithms for many route reconstructions or relay changes and connected status percentage. On the other hand it was seen AEABR and ATAABR improved EABR connection stability by keeping connection outage time low while ATAABR needed less algorithm modification and less computation time.

Trust and Reputation have been used successfully across various networking problems. Reputation for Directory Services (ReDS), a framework to enhance lookups in redundant Distributed Hash Tables (DHTs) by tracking how other nodes service lookup requests was presented by Akavipat, et al.,[13]. ReDS technique could be applied to any redundant DHT including Halo and Kad. The collaborative identification was studied and bad lookup paths removed without relying on shared reputation scores, as such sharing resulted in vulnerability to attacks making it unsuitable for most ReDS applications. Simulations demonstrated that ReDS improved for Halo and Kad by over 80 percent or more on a range of conditions against strategic attackers attempting to game reputation scores and in node churn presence.

A comprehensive investigation on state-of-the-art countermeasures to deal with packet dropping attack was made by Djahel, et al.,[14]. The challenges were also examined to construct an in-depth defence against such sophisticated attacks. Extensions to AODV routing protocol and Adhoc On-demand Multipath Distance Vector (AOMDV) routing protocol were proposed by Li, et al.[15]. It also included a trust-based reactive multipath routing protocol, Adhoc On-demand Trusted-path Distance Vector (AOTDV) for MANETs. This discovered multiple loop-free paths as candidates in a route discovery. Paths were evaluated by hop counts and trust values. Experiments compared these protocols and results reveal that AOTDV improved packet delivery ratio and mitigated impairment from grey hole, black hole and modification attacks.

Stealthy Attack Detection and Countermeasure (SADEC) to detect and isolate stealthy packet dropping attack efficiently was presented by Khalil and Bagchi [16]. SADEC provided a mechanism to utilize local monitoring by increasing nodes number greatly in a neighbourhood which it monitors. A risk-aware response mechanism to cope with identified routing attacks was proposed by Zhao, et al.,[17]. It was based on an extended Dempster-Shafer mathematical theory of evidence, introducing a notion of importance factors. Also, experiments demonstrated effectiveness of the new approach considering many performance metrics.

Trust based routing to avoid untrustworthy nodes was proposed by Xia, et al.,[18]. An adaptive cross-layer routing scheme selecting reliable path was proposed by Anastasopoulos, et al.,[19]. A game theoretical structure for dynamic pricing-based routing in MANETs to maximize sender/receiver quests payoff by considering MANETs dynamic nature was suggested by Ji, et al.,[20]. Toh, et al.,[21] considered dynamic topology in bandwidth constrained environment.

METHODOLOGY

Fuzzy game theory based model and using dwelling selection is described in this work. Game theory development studies, decision making in conflict situations and in cooperation sometimes. Game theory provides a mathematical process to select an optimal strategy[22]. Game theory is applicable to solve decision-making engineering problems.

Game theory provides mathematical tools and models to investigate multi person strategic decision making where players or Decision Makers (DM) compete for limited/ shared resources. Security games study as a special case, interaction between malicious attackers and defenders. Security games and solutions are basis for formal decision making and algorithm development and to predict attacker behaviour. Based on information type available to DMs, action space and DMs goal, security games vary from simple deterministic to more complex stochastic and limited information formulations and are applicable to security problems in various areas from privacy to intrusion detection and cryptography in wireless, computer, and vehicular networks. Game theory is an analytical tool helping researchers design computer networks security protocols. It is a rich mathematical tool to analyse and model new security problems[23]. Moreover, the defender gains a deeper understanding of attacker's strategies through equilibrium analysis of security game as also potential attack risks. Consider

$$\mu_A = \begin{cases} 0,\ when\ A \le a_1, \\ 2\times\left(\dfrac{A-a_1}{a_3-a_1}\right)^2,\ when\ a_1 \le A \le a_2, \\ 1-2\times\left(\dfrac{A-a_3}{a_3-a_1}\right)^2,\ when\ a_2 \le A \le a_3, \\ 1,\ when\ A \ge a_3, \end{cases}$$

where a_1, a_2, a_3 are subjectively selected values. Dependency function is a description of dependence of dependency value's (ì) from options of values (*x*), based on the parameters models ì$_{(x, p)}$.

Fuzzy routing considers uncertainty in routing decisions[24]. In this work the membership functions used are Number of successful deliveries, Memory utilization and computed trust. Based on fuzzy model, a node can find the trust value of its neighbours. The value of trust is lower for malicious nodes compared to legitimate nodes[25].

Trust computations use 'experience', 'recommendation' and 'knowledge'[26] components. Trust measured directly by a node from its neighbors constitute 'experience' component. When the positive experience of a neighbor node is shared, this data is propagated to nodes as 'recommendation' part of the trust. Previously evaluated trust is added to the 'knowledge' component. Trust of node x is calculated by node y is given by

$$T = \sum W(R_i)$$

where W(.) is a weight given to a specific event which may include various misbehavior factors like route request misbehavior, route error misbehavior.

A trust model must suit different situations in a system. In open MANETs, nodes

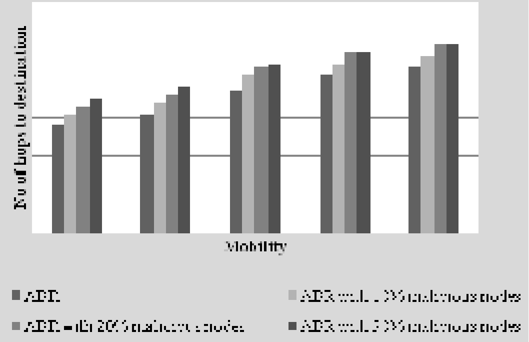

Fig. 1. Number of hops to destination for ABR

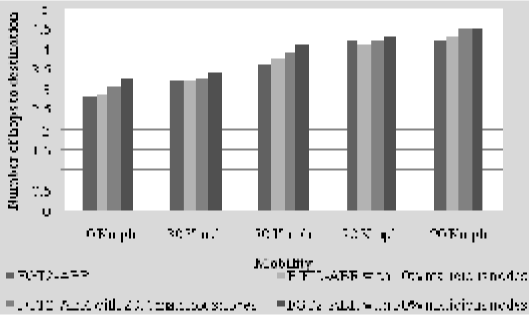

Fig. 2. Number of hops to destination for FGT2-ABR

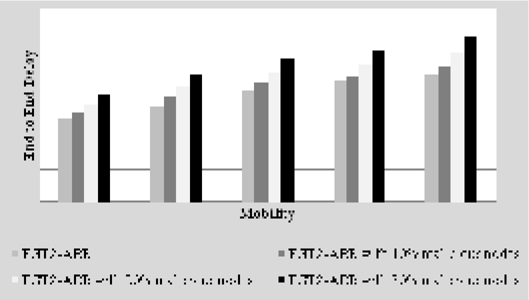

Fig. 4. End to End delay for FGT2-ABR in seco

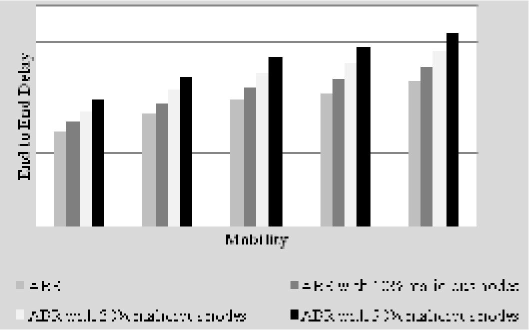

Fig. 3. End to End delay for ABR

may be free to join/leave network anytime. Some nodes may already know each other before joining a network[27]. Besides direct interaction network experience, pre-shared knowledge, is also important for nodes to implement trust evaluation and must be considered accountable experience in a trust model

RESULTS AND DISCUSSION

Simulations were conducted for varying mobility speed using random way point model. Nodes in the network are selected randomly to act maliciously by either control packet dropping or packet dropping. The maliciousness in the network is varied 10%, 20% and 30%. Fifty nodes were used in the simulation with the range of each node being 250 m and the size of the network being 2000 sq.m. ABR and the proposed FGT2-ABR are simulated in these scenarios and its performance with regard to the number of hop count, end to end delay and packet delivery ratio is evaluated. Table 1 shows the results obtained for all the scenarios. Figure 1 shows the number of hops to destination when ABR routing is used for different number of malicious nodes.

It is seen from figure 1 that the Number of hops to destination for ABR increases with the increase in mobility speed and maliciousness due to the frequent packet drops and lost packets. It is seen that the mobility has great impact on the Number of hops to destination, as the mobility increases from 20 to 90 kmph the Number of hops to destination increases by 10.71% to 53.57% when compared with 10 kmph speed in a non-maliciousness network. Figure 2 shows the number of hops to destination using the proposed technique.

It is seen from figure 2 that the Number of hops to destination for the proposed FGT2-ABR increases with the increase in mobility speeds and maliciousness. As mobility increases from 20 to 90 kmph, the number of hops to destination increases by 14.29 to 50% when compared with 10 kmph speed in a non-maliciousness network. The Number of hops to destination increases significantly more in the increase in maliciousness in the network. When compared to ABR, the proposed FGT2-ABR on an average has similar number of hops to destination when the network has no malicious nodes whereas in a malicious network of 30% the proposed FGT2-ABR achieves decreased Number of hops to destination by 6.06 to 11.76% to 3.4% than ABR. Figure 3 shows the end to end delay in seconds for various scenarios.

From figure 3 that the end to end delay for ABR increases with the increase in mobility speed and maliciousness. It is seen that the mobility has great impact on the end to end delay, as the mobility increases from 20 to 90 kmph the end to end delay increases by 7.99% to 52.52% when compared with 10 kmph speed in a non-maliciousness network. The delay increases significantly more as the increase in maliciousness in the network.Figure 4 shows the end to end delay for the proposed technique.

It is seen from figure 4 that the end to end delay for the proposed FGT2-ABR increases with the increase in mobility speed and maliciousness. As the mobility increases from 20 to 90 kmph the end to end delay increases by 5.75% to 51.82% when compared with 10 kmph speed in a non-

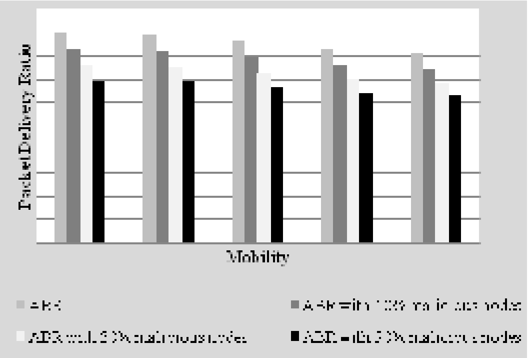

Fig. 5. Packet Delivery Ratio for ABR

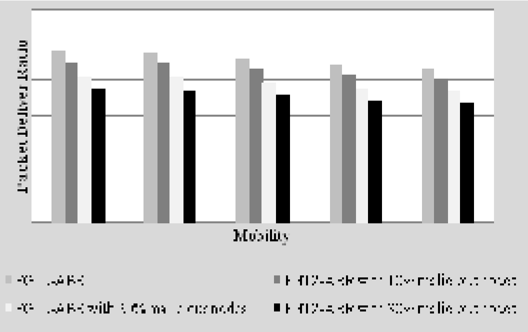

Fig. 6. Packet Delivery Ratio for FGT2-ABR

Table 1. The simulation results for different scenarios of ABR and proposed ABR

Node Mobility in Kmph	ABR	ABR - with 10% maliciousness	ABR - with 20% maliciousness	ABR - with 30% maliciousness	FGT2-ABR	FGT2-ABR with - 10% maliciousness	FGT2-ABR - with 20% maliciousness	FGT2-ABR - with 30% maliciousness
No of hops to destination								
10	2.8	3.1	3.3	3.5	2.8	2.9	3.1	3.3
30	3.1	3.4	3.6	3.8	3.2	3.2	3.3	3.4
50	3.7	4.1	4.3	4.4	3.6	3.8	3.9	4.1
70	4.1	4.4	4.7	4.7	4.2	4.1	4.2	4.3
90	4.3	4.6	4.9	4.9	4.2	4.3	4.5	4.5
End to End Delay								
10	0.0514	0.0566	0.0624	0.0688	0.0521	0.0555	0.0606	0.0667
30	0.0608	0.067	0.0738	0.0813	0.0596	0.0652	0.0716	0.0788
50	0.0684	0.0754	0.0831	0.0916	0.0692	0.0733	0.0806	0.0886
70	0.0726	0.08	0.0882	0.0972	0.0748	0.0777	0.0855	0.0939
90	0.0784	0.0864	0.0952	0.1049	0.0791	0.0839	0.0923	0.1014
Packet Delivery Ratio								
10	0.90278	0.8279	0.7593	0.6964	0.9715	0.9056	0.8254	0.7534
30	0.8948	0.8206	0.7526	0.6902	0.9599	0.896	0.8179	0.7466
50	0.8642	0.7926	0.7269	0.6666	0.9245	0.8652	0.7896	0.7199
70	0.8321	0.7631	0.6998	0.6418	0.89	0.8309	0.7585	0.6915
90	0.8144	0.7469	0.685	0.6282	0.8709	0.8132	0.7414	0.676

maliciousness network. The delay increases significantly more in the increase in maliciousness in the network. When compared to ABR, the proposed FGT2-ABR has more end to end delay in the range of 0.89% to 3.03% when the network has no malicious nodes whereas in a malicious network of 30% the proposed FGT2-ABR achieves decreased delay of 3.05% to 3.4% than ABR. Figure 5 shows the Packet Delivery Ratio (PDR) for ABR.

It is observed from figure 5 that the packet delivery ratio for ABR decreases with the increase in mobility speed and maliciousness. As the mobility increases from 20 to 90 kmph the packet delivery ratio decreases by 2.13% to 9.79% when compared with 10 kmph speed in a non-maliciousness network. The packet delivery ratio decreases significantly more in the increase in maliciousness in the network.Similarly figure 6 shows the PDR of the proposed technique.

It is observed from figure 6 that the packet delivery ratio for proposed FGT2-ABR decreases with the increase in mobility speed and maliciousness. As the mobility increases from 20 to 90 kmph the packet delivery ratio decreases by 2.15% to 10.36% when compared with 10 kmph speed in a non-maliciousness network. The packet delivery ratio decreases significantly more in the increase in maliciousness in the network. When compared to ABR, the proposed FGT2-ABR has better packet delivery ratio in the range of 6.94% to 7.61% when the network has no malicious nodes whereas in a malicious network of 30% the proposed FGT2-ABR achieves higher packet delivery ratio of 7.61% to 8.18% than ABR.

CONCLUSION

In this work Fuzzy game theory was used for route selection. Membership functions in this work are Number of successful deliveries, Memory utilization and computed trust. Trust is based on neighbourhood trust and recommendation based trust. Experiments were conducted in varied scenarios using ABR and the new method. Results showed the proposed approach's improved performance regarding packet delivery ratio. The new FGT2-ABR had better packet delivery ratio ranging between 6.94% and 7.61% when network has no malicious nodes while in a malicious network of 30% the new3 FGT2-ABR achieved higher packet delivery ratio ranging between 7.61% and 8.18% than ABR. Further investigations are needed to reduce end to end delay which is slightly higher in the proposed technique.

REFERENCES

1. Zhao, Z., Hu, H., Ahn, G. J., and Wu, R. Risk-Aware Mitigation for MANET Routing Attacks. Dependable and Secure Computing, *IEEE Transactions on*, 2012; **9**(2), 250-260.
2. Aarti and S.S. Tyagi.. Study of MANET: Characteristics, Challenges, Application and Security Attacks. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2013; **3**(5), pp 252-257.
3. Milanovic, N., Malek, M., Davidson, A., and Milutinovic, V. Routing and security in mobile ad hoc networks. *Computer*, 2004; **37**(2), 61-65.
4. Ghosekar, P., Katkar, G., and Ghorpade, P. Mobile ad hoc networking: imperatives and challenges. IJCA special issue on "Mobile ad hoc networks", MANETs 2010.
5. Sastry, V. N., and Supraja, P. Location-based associativity routing for MANET. In Wireless And Mobile Computing, Networking And Communications, 2005.(WiMob'2005), *IEEE International Conference on* 2005; **3**: pp. 49-56
6. Masoud, F. A., Shaar, S. A., Murad, A., and Kanaan, G. Enhanced route re-construction method for associativity based routing protocol for Mobile Ad hoc Networks (MANET). *Journal of Computer Science*, 2006; **2**(12): 859.
7. Toh, C. K. Associativity-based routing for ad hoc mobile networks. *Wireless Personal Communications*, 1997; **4**(2): 103-139.
8. Manikandan, S., Naveenan, R., Padmanaban, R. K., and Ramachandran, V. Optimized associativity-based threshold routing for mobile adhoc networks. In 8th International Conference on High Performance Computing (HiPC'2001), Hyderabad, India 2001.
9. Preveze, B., and Safak, A. (2009, November). Associativity tick averaged associativity based routing (ATAABR) for real time mobile networks. In Electrical and Electronics Engineering, 2009. ELECO 2009. International Conference on (pp. II-208). IEEE.
10. Murad, A. M., Al-Mahadeen, B., and Murad, N. M. (2008, December). Adding Quality of Service Extensions to the Associativity Based Routing Protocol for Mobile Ad Hoc Networks (MANET). In Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE (pp. 631-

637). IEEE.

11. Heo, G., and Song, W. C. (2009, January). Associativity-based dynamic source routing in MANETs. In Information Networking, 2009. ICOIN 2009. International Conference on (pp. 1-3). IEEE.
12. Preveze, B., and Safak, A. (2010, September). Comparative analysis of novel long life routing methods in mobile networks. In Personal Indoor and Mobile Radio Communications (PIMRC), 2010 IEEE 21st International Symposium on (pp. 1596-1601). IEEE.
13. Akavipat, R., Al-Ameen, M. N., Kapadia, A., Rahman, Z., Schlegel, R., and Wright, M. (2012). ReDS: A Framework for Reputation-Enhanced DHTs. arXiv preprint arXiv:1209.4867.
14. Djahel, S., Nait-Abdesselam, F., and Zhang, Z. Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges. Communications Surveys and Tutorials, *IEEE,* 2011; **13**(4): 658-672.
15. Li, X., Jia, Z., Zhang, P., Zhang, R., and Wang, H. Trust-based on-demand multipath routing in mobile ad hoc networks. *Information Security, IET,* 2010; **4**(4): 212-232.
16. Khalil, I., and Bagchi, S. Stealthy attacks in wireless ad hoc networks: detection and countermeasure. Mobile Computing, *IEEE Transactions on,* 2011; **10**(8): 1096-1112.
17. Zhao, Z., Hu, H., Ahn, G. J., and Wu, R. Risk-Aware Mitigation for MANET Routing Attacks. Dependable and Secure Computing, *IEEE Transactions on,* 2012; **9**(2): 250-260.
18. Xia, H., Jia, Z., Ju, L., and Zhu, Y. Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory. *Wireless Sensor Systems, IET,* 2011; **1**(4): 248-266.
19. Anastasopoulos, M. P., Arapoglou, P. D., Kannan, R., and Cottis, P. G. Adaptive routing strategies in IEEE 802.16 multi-hop wireless backhaul networks based on evolutionary game theory. Selected Areas in Communications, *IEEE Journal on,* 2008; **26**(7): 1218-1225.
20. Ji, Z., Yu, W., and Liu, K. R. A game theoretical framework for dynamic pricing-based routing in self-organized MANETs. Selected Areas in Communications, *IEEE Journal on,* 2008; **26**(7): 1204-1217.
21. Toh, C. K., Guichal, G., and Bunchua, S. Abam: On-demand associativity-based multicast routing for ad hoc mobile networks. In Vehicular Technology Conference, 2000. IEEE VTS-Fall VTC 2000. 52nd (Vol. 3, pp. 987-993). IEEE.
22. Medineckiene, M., Zavadskas, E. K., and Turskis, Z. Dwelling selection by applying fuzzy game theory. *Archives of Civil and Mechanical Engineering,* 2011; **11**(3), 681-697.
23. Manshaei, M., Zhu, Q., Alpcan, T., Basar, T., and Hubaux, J. P. Game theory meets network security and privacy. *ACM transaction on Computational Logic,* 2011; **5.**
24. Dai, H., Jia, Z., and Qin, Z. Trust evaluation and dynamic routing decision based on fuzzy theory for manets. *Journal of Software,* 2009; **4**(10): 1091-1101.
25. Wang, X., Wu, Y., Ren, Y., Feng, R., Yu, N., and Wan, J. An Evolutionary Game-Based Trust Cooperative Stimulation Model for Large Scale MANETs. International Journal of Distributed Sensor Networks, 2013.
26. Govindan, K., and Mohapatra, P. Trust computations and trust dynamics in mobile adhoc networks: a survey. Communications Surveys and Tutorials, *IEEE,* 2012; **14**(2): 279-298.
27. Li, X., Slay, J., and Yu, S. Evaluating trust in mobile ad hoc networks. In The Workshop of International Conference on Computational Intelligence and Security 2005.
28. B. Akay and D. Karaboga, “Parameter tuning for the artificial bee colony algorithm,” in Proceeding of the 1st International Conference on Computational Collective Intelligence (ICCCI ’09), pp. 608–619,Wroclaw,Poland, 2009.