Acta Technica *62* No. 1B/2017, 45–56

Security dynamic performance evaluation method of ad hoc network based on anti-attack model

Xiaoling Xu[1], Weicui[2,3], Tianyun Zhang[1]

Abstract. The purpose of this paper is to study the security of Ad hoc networks. The Ad hoc network is decentralized and self-organized. It has the unique characteristics of topological dynamic change and fully open wireless access. They are easily attacked by various network malicious nodes. Based on the anti - attack model, the security of Ad hoc network is analyzed. By using the model, the corresponding trust filtering mechanism is established. It can detect nodes stably. At the same time, the recommended nodes and nodes with collusion attack are found in the link. Through the theoretical analysis and experimental simulation, the results show that the proposed model can avoid the attack of malicious nodes, so as to realize the stable operation of the whole system. Based on the above findings, we conclude that this model can effectively solve the trust management problem in Ad hoc networks.

Key words. Anti-attack model, Ad hoc, network security, trust in peers.

1. Introduction

Ad hoc network is a kind of temporary autonomous distributed system in terms of its system, which shows a lot of natural disadvantages in the practical application. There are many problems that need to be solved urgently, among which the problem of network security is remarkable since without solution, it would be difficult to achieve the universal application of network, while the security of network node has always been one of the important issues conducted in research [1]. With the Ad hoc network model continuing to enter into thousands of households, how to better improve the security of Ad hoc system is one of the main problems that is in need to be solved. Some studies have indicated that the real-time monitoring of node control and the interception of malicious nodes in the network are gradually becoming the main methods to enhance the service capability of Ad hoc network [2].

[1]Information Network Center, Lanzhou City University, Lanzhou, 730070, China
[2]Educational Administration Office, Lanzhou Jiaotong University, Lanzhou, 730070, China
[3]Corresponding author

Meanwhile, the anti-attack model has gradually become the mainstream of research. This model, in the process of research, with direct access to the communication nodes in the whole system, ensures the smooth development of the entire system, which follows a specialized trust evaluation of nodes [3].

Usually, the wireless communication network mainly refers to the cellular mobile communication system or the wireless. The former usually adopts centralized centralized control mode, and needs related infrastructure support, such as base station or switch. The latter is connected to the fixed network in a wireless access mode. What they all have in common is that mobile terminals require fixed network support. However, these are not suitable for certain occasions. Therefore, we urgently need a ubiquitous network, that is, mobile Ad hoc networks. Mobile Ad hoc network is a new type of wireless network. It does not depend on the control of the fixed infrastructure, but emphasizes the concept of multi hop, self-organization and no center. Nodes in a network have dual roles. It has both router function and host characteristics, which are connected as peer entities. The normal communication process between nodes must be relayed by other nodes in the network, so as to construct a multi hop wireless network. Although mobile Ad hoc network has many advantages, such as fast, flexible and strong invulnerability, it has many inherent security problems, such as no linearity, dynamics, self-organization and resource limitation. Therefore, its security has become a serious challenge for mobile Ad hoc network research. As a kind of computer network, the network also has to solve the basic network security problems, such as the availability of basic network services, the confidentiality of information and the integrity of network information. Authentication, communication, encryption and authorization are the main means to achieve the above goals. The specific methods include authentication protocol, digital signature, information encryption and so on. These methods still play an important role in ensuring the availability, integrity, authentication, and non-repudiation of network communications. However, these mechanisms require nodes with higher hardware requirements. As a result, its actual operation is relatively inefficient. In addition, security mechanisms in centralized networks are not suitable for mobile Ad hoc networks. It cannot prevent unsafe behavior, malicious behavior and selfish behavior in the network. In this network, the mutual trust between nodes is of great importance to the security and reliable operation of the network. The establishment of trust relation is the premise of normal communication. In order to establish security communication, a perfect trust model must be established among the nodes, and it is one of the main means to solve malicious attacks in the network by determining the trust relationship between nodes. Therefore, the research of mobile Ad hoc network trust model is a direction to solve the problem of network soft security. However, mobile Ad hoc network is a resource constrained autonomous system. Because nodes are controlled and used by many rational users, the nodes in the network often show their privacy. In the normal packet forwarding process, it is not willing to actively provide services for other nodes, which results in a dramatic decline in network performance. Therefore, in this environment, it is another direction to solve the problem of network soft security by motivating and mobilizing the cooperation enthusiasm of selfish nodes. At present, the research on secure routing

of mobile Ad hoc networks is based on table driven, on-demand and hybrid routing protocols. Security enhancement is carried out by using the idea of hard security. The introduction of trust and cooperation mechanisms provides a new approach for solving the soft routing problem in mobile Ad hoc networks.

The security protection of network is achieved in trust evaluation where the system attacks directly malicious nodes for the invasion into the system, thereby expelling these nodes out of the system. After the relevant research and evaluation of this problem, the preliminary analysis shows that in the network communication security, if the trust is increased or remain unchanged among these nodes with better behaviors, then the other nodes in the network will be more willing to carry out communication [4], on the contrary, the trust of these nodes with poor behaviors will continue to decline, and the other nodes will exclude or even refuse the communication with them. Where, the process seems to imitate the new relationship of new person in human society, with its operation model involving hypothesis, expectations and the corresponding behavior and environment, which are more appropriate to conform to the human social relations [5]. At the same time, the trust evaluation model is also an important driving force of the whole anti-attack model, which prevents the network from being attacked internally, and is suitable for distributed network communication [6]. In the actual use, it can strengthen the detection of malicious nodes to improve the security of the system [7], so the trust evaluation system has also gradually become the focus in researches on the security of Ad hoc network based on anti-attack model [8]. With the continuous development and progress of Ad hoc network's applications, how to establish the trust relationship between unrelated individuals is also the most important issue [9].

2. State of the art

In the simulation of Ad Hoc network, most people use mobile model (MM) based on single entity, such as RWPM (random waypoint mobility model), RWM (random walk mobility model), RDM (random direction mobility model) and GMMM (Gauss–Markov mobility model). RWPM is the basic model, and the most commonly used MM. In RWPM, the MN randomly takes the starting point S and the destination point D in the moving area, and randomly takes the velocity v and moves from S to D in a straight line. After MN arrives at D, randomly select a pause time to remain stationary, thus completing a step. Then, the next round step movement is performed with the present round destination point D as the start point S of the next movement, and the other MNs follow the above-described movement pattern and move independently of each other. Other models are mostly evolved from RWPM, when the pause time of MN in RWPM is zero, RWPM becomes RWM. RWM will produce unrealistic dynamic characteristics, such as sudden stop and sharp turn. RDM reduces the node density fluctuation on the basis of RWPM, but it cannot improve the network topology connectivity performance under RWPM. GMMM is based on the use of the RWPM Markov chain to establish the movement model, it attempts to describe a more realistic movement pattern, but due to MN in some direction cannot change the speed of movement, resulting in the dynamic

characteristics of the network is still flawed (such as node location distribution, etc.).

The EMWMSDP evaluation method proposed in this paper can quantitatively evaluate the temporal and spatial dynamic characteristics of interrelated MM. On this basis, the CCMM model is also proposed to describe the curve movement model with realistic scene. For simplicity, it is assumed that the MN moves within a circular region, but it can be extended to other moving regions (such as rectangles) and can quantitatively compare the temporal and spatial dynamics of different MM. Because the method is independent of any MM, the results of Ad Hoc network-related research (such as protocol optimization and performance evaluation) under different MMs are comparable and the conclusion is more reliable. In addition, the EMWMSDP method can evaluate the temporal and spatial dynamic characteristics of MM more comprehensively and make up for the deficiency of single dynamic characteristic research. In the Ad Hoc network, the network model describes and reflects the geometric characteristics of the mobile node (MN), such as the mode of motion, speed and direction, which is the main factor of the network topology change. In the existing research of Ad Hoc networks (such as MAC protocol and routing protocol optimization, network performance prediction, etc.) are often based on a specific model for the premise. The network model makes the Ad Hoc network show complex dynamic characteristics (such as the spatial distribution of node location, the duration of network link connectivity, etc.) both in time and space. Most of the existing models are based on simple, random (or blind) linear motion, it not only difficult to describe the reality of the curve of motion patterns, but also produce such as the border effect (border effect), speed attenuation and other defects, resulting in the simulation based on these models can not accurately reflect the real network behavior, it is necessary to establish a mobile model close to reality. However, how to analyze the dynamic characteristics and simulation results of different models of Ad Hoc network systematically and comprehensively, and theoretically require a general and quantifiable evaluation method [10]. At present, most of the researches on dynamic characteristics of mobile models are based on the moving model itself and its one side (such as temporal or spatial dynamic) to establish a specific computing model. It is difficult to be independent of the mobile model, because it is difficult to independent of the mobile model, so the lack of comparability and versatility [11].

In the network, trust and security are two different concepts. Security is mainly based on the security of the system. It can avoid or deal with illegal intrusions, malicious attacks and so on. However, in the current network, trust is to help the network entity to establish confidence or judge service cooperation, to reduce the risk and substantive cooperation [12]. At the same time, the two are closely related. Security can provide reliable communication and information protection for the creation of trust, and trust can enhance security. In order to correctly distinguish selfish nodes and malicious nodes on the network, many scholars have proposed the establishment of a trust model and the routing algorithm according to the history of interactions between entities, to achieve node priority trust, as well as the normal communication [13]. The weight of the score is determined by the confidence, credibility, timing, score, and distance of the existing scoring. This method overcomes the disadvantages of the simple trust model, which is too

rough to describe the trust value accurately, and the algorithm is simple, intuitive and easy to understand [14]. The method of probability theory is more suitable for the requirement of historical interaction information collection in trust model. Beth first divides trust into direct trust and recommendation trust, calculates trust value by probability statistics, and proposes a method for synthesizing trust. The trust value is evaluated by calculating the binary probability or positive conditional probability value. However, it does not consider the nature of trust and decay over time. Bias network is based on the Bias theorem in probability theory, and is one of the common methods of uncertainty reasoning. It provides an accurate theoretical basis for calculating trust value [15]. In its calculation, the prior probability, the sufficiency measure, the necessity measure and the equivalence are mostly given by expert experience. Some papers call it the Subjective Bayes approach. However, this method relies too much on expert experience and is more subjective. It is difficult to implement in Ad hoc network [16]. The uncertainty of trust is expressed by entropy, and the model also calculates the direct trust value between entities based on Bayesian theory, and takes into account the factors that decay with time. However, the proposed model does not consider more than two recommended trust synthesis problems. It does not satisfy the combination rate of trust synthesis. It cannot deal with trust recommendation from multiple parties, and does not distinguish direct trust from indirect trust.

In the model proposed by George et al., the trust evaluation problem is considered as the shortest path problem of weighted directed graph trust graphs, using path based semi loop and distance based semi loop transfer and composite trust respectively [17]. The trust of the model is only based on the demand of intuitive subjective judgment, and lacks the proof of the theoretical basis of the evidence. Moreover, the trust is generated only on the basis of local observation, so the amount of information needed for the calculation of trust is not complete enough. Luo Junhai proposed a trust model based on strategy game. The trust relationship among nodes is modeled. It gives the corresponding node's policy selection and payment function, thus ensuring that the trust model can identify malicious nodes, ensure secure communication between trusted nodes, and improve the performance of the network. Combining the concept of trust, Zhang Tao proposed the modeling idea of routing algebra. Based on this, we define and quantify the routing metric metrics in current trust routing research, and validate the idea theoretically, and extend the model to other classic routing protocols. This method is the first to give a complete set of theoretical systems about trust routing, and it has also a very good scalability [18]. The dynamic, time-varying and lost characteristics of wireless links lead to poor quality and low stability of wireless links, which challenges the reliability of network throughput and transmission. In addition, the link instability caused by node mobility and the limited energy of nodes also make it difficult to design and optimize routing protocols. However, broadcast characteristics of wireless channels are inherent advantages. Opportunistic routing takes advantage of this characteristic of wireless channels to improve the transmission reliability and end-to-end throughput of wireless networks.

3. Methodology

3.1. Synthetic update of direct trust

In the ubiquitous environment, the nodes in the network can form a network with relatively stable topology at extremely fast speed. In this process, the nodes, mainly through the sharing of services and the cooperation of equipment, complete the function between each other, which can also primarily realize the application of a variety of mobile business with the use of self-organizing network [19]. While, it is necessary to be based on self-organizing network nodes for the application so as to achieve a variety of service resources by cooperating with request nodes. However, in the actual working environment, owing to their own limited resources, nodes would become selfish nodes or nodes with malicious strategy [20].

Among these nodes, selfish nodes, which would lead to the emergence of various problems of the entire system, directly determine the stability and security of the entire system [21]. For a server, if the number of selfish nodes is excessive, it will have a great adverse impact on excellent nodes in the network for its combating the enthusiasm of these excellent nodes to provide services, which directly causes the difficulty of the entire network in continuing [22]. Furthermore, the selfish node—Free-Rider also has a huge adverse impact in the network layer where misbehavior nodes attain its selfish purpose for their avoiding to provide the appropriate services, or packet forwarding services for other nodes. Thus, if these selfish nodes exist longer in the system, the destructive degree to system will become greater, meanwhile, exerting serious impact on the normal operation of system communication [23].

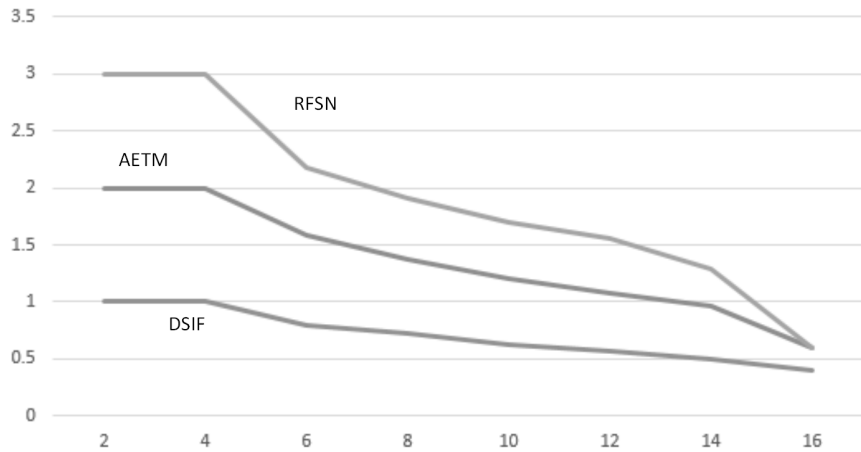

Fig. 1. Strategic attack of 1000 nodes under the change of direct trust

In the application, direct trust is based on the accumulation in interactive records of service request nodes and target nodes, and further provides strong evidence for the trust evaluation of the entire system, as shown in Fig. 1. Here, RFSN is reputation-based framework for sensor networks, AETM is ad-hoc enabled trust

mechanism and, DSIF is dynamic sensor information fusion. The trust relationship established between two different nodes is the direct trust between these two nodes, which is mainly regarded as the degree of trust to the target nodes that have experienced in the services for request nodes according to its actual needs [24], with its significant importance for the safe operation of the entire system.

3.2. Design principles of incentive mechanism

The incentive subject interacts with the incentive object, during which the process is reflected through a series of rationalized incentive mechanisms. In the practical application, the main rules of the incentive mechanism are as follows: First of all, one of the most important rules is open and intuitive principle, under which, purposes with the need to be incentive as well as methods require to be extremely clear, intuitive and open, so as to satisfy the open and intuitive principle of the entire system. Thus, the openness and intuitiveness of incentive mechanism is the primary link with significant focus when designing the network.

Secondly, it is the principle of objectives' combination that requires determination of goals of the whole mechanism with needs to be considered in the design process. However, in the construction of the network system, it is necessary to meet the individual requirements of participants for the realization of this link. In these processes, tangible and intangible incentives participating in activities together in the entire system will adopt different approaches to carry out classified incentives in different situations, thereby ensuring the balance and stability of the entire system for its long-term development and the maintenance of system's security.

Thirdly, the principle is praising virtue and punishing vice. Based on this principle, through incentive mechanism, participants who participate in the entire system would give up those behaviors that are harmful to the development and security of the system, and those who carry out reasonable operations and maintain the security would be further rewarded. In the actual incentive mechanism, the participants who are in accordance with target behaviors should be rewarded, and those who compromise the stability of system should be sanctioned from another point of view, as shown in Fig. 2. The symbols α and β represent the adaptability of 2 kinds of behavior compromises of the system. The symbol γ represents the adaptability of the incentive behavior.

The forth principle is to be incentive on demand, that is, the incentive mechanism must be based on its meeting the needs of nodes in the system. However, in different period of time, it is often different from the leading of stage nodes, so it is indispensable to meet the most urgent need in all needs of nodes in order to make these incentives can be carried out to the greatest extent.

The last one is the effectiveness principle of the system, which helps more nodes in incentive system to further bring about positive behaviors that are in line with the overall interests. At the same time, in order to effectively prevent those behaviors that do not meet the requirements and those violating the interests, the whole incentive mechanism can better promote the timely implementation of this part of punitive measures.

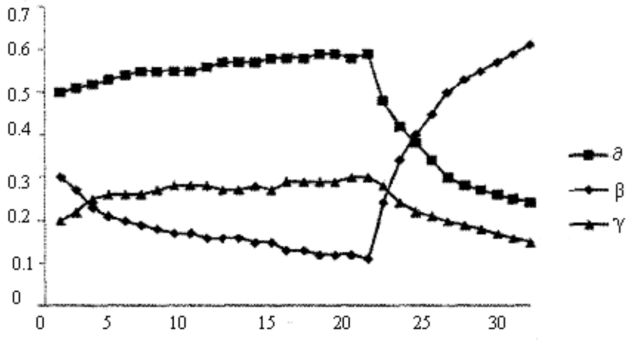

Fig. 2. Dynamic adaptability analysis

3.3. Analysis of simulation experiment

In the analysis of this problem, the source node, based on its own node, directly select the value of trust to send node's service request. The results are shown in Fig. 3. In the whole system, it is illustrated that all nodes have their own needs and rationality, desiring to choose a node with a higher trust value to provide more stable and reliable service. Thus, this part of excellent nodes with high value of trust, in the actual participation, often select those nodes that have the same good characteristic, so as to ensure that good nodes tend to combine with other good nodes for the stability of the entire system. Therefore, excellent nodes can be gradually gathered together to form a more solid network, so that all nodes within the region can obtain reliable network services, finally achieving the upgrade of priority. For those nodes with extremely low contribution rate and that are harmful to the stable development of the entire system, the anti-attack model is applied to eliminate them, and the malicious nodes are identified and cleared accordingly to ensure that all nodes are excellent, while to avoid the entering of many malicious nodes. Thus, the security and stable development of the network will gradually be achieved. Similarly, the request information sent by many nodes with malicious strategy, which is used by selfish nodes and malicious nodes can only be passed within the edge of the network, thus an incentive effect is available for the entire network where a successful interaction that is reliable and with relatively long-term adherence must be provided at the same time, if nodes in network want to get more superior web services.

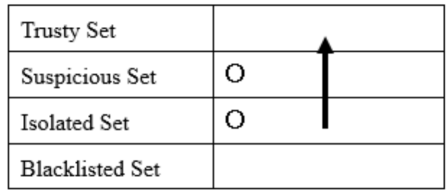

Fig. 3. Transition from an isolated set to a suspect set

In this study, the ability to resist malicious nodes of the entire network was mainly analyzed. The results are shown in Fig. 4. Among these nodes, one kind of node itself will attack maliciously in order to deceive other nodes in the network. Meanwhile, with it disguised itself as benign nodes of this system in the beginning to provide services, as soon as the trust is accumulated to a certain level, it will attack other nodes with the probability to damage the system. In the experiment, in order to further analyze the whole data model in depth, a service requesting node has been designed for the whole system according to various analysis models. In addition, a cheating node is designed for further analyzing how these two nodes participate in activities and how the cheating node obtain the trust in the system, thus it will be more convenient for malicious node to do its own malicious attacks. In these researches on model, the experiment is carried out under the same experimental conditions. The service request node sends 10 times of service request to the malicious node, among which the first three times allow the malicious node to provide the system with relatively stable reliable services, and provide unreliable services for the subsequent seven times.

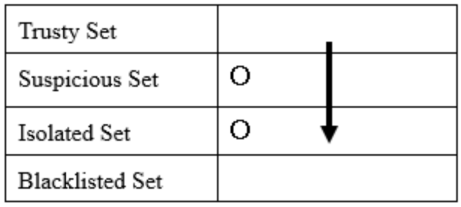

Fig. 4. Node from suspicious set to isolated set conversion

4. Result analysis and discussion

4.1. Design of discount factor

When designing and studying the whole system, the corresponding relationship analysis with D-S evidence theory illustrated that when the evidences are in conflict, if the consistency of some part of evidence is low compared with that of other evidences accounting for the majority, the impact of this part of evidence needs to be reduced to prevent the final fusion results being affected in varying degrees. On the contrary, if the evidence itself is highly consistent with other evidences in the entire system, thus this evidence can be caused corresponding attention in the network transmission, with direct impact on the final fusion results. In the analysis and research, through the comparison and analysis, it was found that in the process of integration, the weight that the evidence assigned to should be proportional to the assigned weight in the integration with other evidences. In this study, the relevant similarity matrix is applied to analyze these data, during which the data relationship is gradually clear, with effectively guaranteeing the accuracy of information every part obtained.

4.2. Proportion of malicious nodes' finding

As for the proportion of malicious nodes, a more detailed data analysis and research is conducted. Through the comparison of data, it was illustrated that not only a kind of malicious node exists in the network, but many kinds of combination of malicious nodes with mutual influence and work together, if assuming that there are 500 malicious nodes. In the further analysis of this study, it was found that the data of different types of nodes among these malicious nodes is in a state of balance, and the proportion is relatively balanced, contributing to the further observation and analysis of these nodes in the experiment (see Fig. 5).

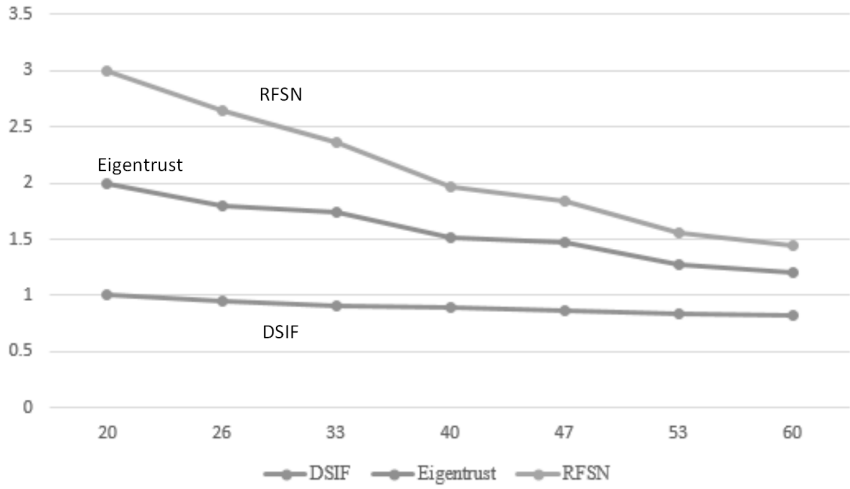

Fig. 5. Relationship between the success rate and the proportion of collusion nodes

In this experimental study, the probability of malicious nodes to be found has been greatly improved based on the research model, which will show a higher level after oscillating reactions. On the basis of this model, the errors caused by the prior distribution of RFSN can be well avoided, and the impact of subjective ambiguity can be more accurately identified, thus maximizing the accuracy of trust evaluation.

5. Conclusion

In this paper, the research on the main link in the trust management of Ad hoc network is conducted, and with it regarded as the background, the anti-attack model is analyzed. Because the network lacks the relative centralized server, and the trust of nodes must be completed by themselves, meanwhile, due to the changes in the network topology and its infinite conflict, some problems existing in the trust evaluation of the system are caused into fact. Then, in the process of establishing the trust evaluation model with the background of evidence theory, the randomness and subjective uncertainty when processing assessment do not require the analysis

of prior distribution. With this model, the relevant trust filtration mechanism can be carried out to detect nodes stably, while the recommended nodes and nodes with collusion attack are found in this link. In this paper, with theoretic analysis and results analysis in simulation, it was found that attacks of malicious nodes can be well avoided to achieve the stable operation of the entire system.

References

[1] V. Pahal, S. Kumar: *Degradation of ad-hoc network performance under wormhole attack.* International Journal of Computer Applications *49* (2012), No. 13, 25–29.

[2] G. M. Borkar, A. R. Mahajan: *A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks.* Wireless Networks (2016), 1–18.

[3] H. C. Chen: *TCABRP: A trust-based cooperation authentication bit-map routing protocol against insider security threats in wireless ad hoc networks.* IEEE Systems Journal *11* (2017), No. 2, 449–459.

[4] M. J. Faghihniya, S. M. Hosseini, M. Tahmasebi: *Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network.* Wireless Networks (2016), 1–12.

[5] A. Hinds, M. Ngulube, S. Zhu, H. Al-Aqrabi: *A review of routing protocols for mobile ad-hoc networks (MANET).* International Journal of Information and Education Technology *3* (2013), No. 1, 1–5.

[6] D. Saravanan, R. M. Chandrasekaran, B. V. Prabha, V. R. Sarma Dhulipala: *Trust worthy architecture implementation for mobile ad hoc networks.* International Journal on Computer Science and Engineering *3* (2011), No. 7, 2601–2609.

[7] W. Li, H. Song: *ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks.* IEEE Transactions on Intelligent Transportation Systems *17* (2016), No. 4, 960–969.

[8] M. Mohanapriya, I. Krishnamurthi: *Trust based DSR routing protocol for mitigating cooperative black hole attacks in ad hoc networks.* Arabian Journal for Science and Engineering *39* (2014), No. 3, 1825–1833.

[9] R. Chen, J. Guo, F. Bao, J. H. Cho: *Trust management in mobile ad hoc networks for bias minimization and application performance maximization.* Ad Hoc Networks *19* (2014), 59–74.

[10] H. Xia, Z. Jia, X. Li, J. Lei, E. H. M. Sha: *Trust prediction and trust-based source routing in mobile ad hoc networks.* Ad Hoc Networks *11* (2013), No. 7, 2096–2114.

[11] R. A. Shaikh, A. S. Alzahrani: *Intrusion-aware trust model for vehicular ad hoc networks.* Security & Communication Networks *7* (2014), TOC No. 11, 1652–1669.

[12] A. Shabbir, F. Khalid, S. M. Shaheed, J. Abbas, M. Zia-Ul-Haq: *Security: A core issue in mobile ad hoc networks.* Journal of Computer Science & Communications *3*, (2015), No. 12, 41–66.

[13] Z. Movahedi, Z. Hosseini, F. Bayan, G. Pujolle: *Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey.* IEEE Communications Surveys & Tutorials *18* (2016), No. 2, 1287–1309.

[14] E. da Silva, L. C. P. Albini: *SEMAN: A novel secure middleware for mobile ad hoc networks.* Journal of Computer Networks and Communications (2016), paper 3136853.

[15] S. Sicari, A. Rizzardi, L. A. Grieco, A. Coen-Porisini: *Security, privacy and trust in internet of things: The road ahead.* Computer Networks *76* (2015), 146–164.

[16] S. Tan, X. Li, Q. Dong: *A trust management system for securing data plane of ad-hoc networks.* IEEE Transactions on Vehicular Technology *65* (2016), No. 9, 7579 to 7592.

[17] D. Lavrova, A. Pechenkin: *Applying correlation and regression analysis to detect security incidents in the internet of things.* International Journal of Communication Networks and Information Security *7* (2015), No. 3, 131–131.

[18] R. Aaseri, P. Choudhary, N. Roberts: *Trust value algorithm: A secure approach against packet drop attack in wireless ad-hoc networks.* International Journal of Network Security & Its Applications (IJNSA) *5* (2013), No. 3, 99–111.

[19] B. Balaji, M. H. Khan, T. S. N. Murthy: *A defense mechanism for EOLSR against DOS attacks in ad hoc networks using trust based system.* International Journal of Security and Its Applications [SCOPUS] *8* (2014), No. 5, 51–64.

[20] F. Zhang, Z. P. Jia, H. Xia, X. Li, E. H. M. Sha: *Node trust evaluation in mobile ad hoc networks based on multi-dimensional fuzzy and Markov SCGM(1, 1) model.* Computer Communications *35* (2012), No. 5, 589–596.

[21] T. Eissa, S. A. Razak, M. A. Ngadi: *A novel lightweight authentication scheme for mobile ad hoc networks.* Arabian Journal for Science and Engineering *37* (2012), No. 8, 179–2192.

[22] R. Venkataraman, M. Pushpalatha, T. R. Rao: *Regression-based trust model for mobile ad hoc networks.* IET Information Security *6* (2012), No. 3, 131–140.

[23] Z. Yan, P. Zhang, A. V. Vasilakos: *A survey on trust management for internet of things.* Journal of Network and Computer Applications *42* (2014), 120–134.

[24] M. Kaliappan, B. Paramasivan: *Enhancing secure routing in mobile ad hoc networks using a dynamic bayesian signalling game model.* Computers & Electrical Engineering *41* (2015), 301–313.

Received June 29, 2017