A novel secure routing scheme using probabilistic modelling for better resistivity against lethal attacks

Jyoti Neeli[1], N. K. Cauvery[2]
[1]Department of Information Science and Engineering, Global Academy of Technology,
Visvesvaraya Technological University (VTU), India
[2]Department of Information Science of Engineering, RV College of Engineering,
Visvesvaraya Technological University (VTU), India

Article Info

Article history:

Received Jul 10, 2019
Revised Feb 29, 2020
Accepted Mar 18, 2020

Keywords:

Attack
Intrusion
Malicious
Secure routing
Security
Wireless adhoc network

ABSTRACT

Study towards wireless adhoc network dates two decades back with various researchers evolving up with new solutions towards addressing its problems. Irrespective of various other problems, the issues related to the secure routing is yet unsolved owing to massively increasing fatal strategies of the adversary. Review of existing literature shows that the existing secure routing scheme can only govern over the stated attacks reducing the applicability in case of dynamic attacks. Therefore, this manuscript introduces a novel probabilistic model which offers the capability to wireless nodes to identify the malicious behavior and react accordingly. Different from existing intrusion prevention system, the proposed system allows the malicious node to participate in the data forwarding process and exhaust its resources with no chance of launching an attack. The simulated outcome of the study shows that the proposed secure routing scheme offers better data forwarding characteristic in contrast to the existing system in the aspect of intrusion detection and secure data transmission.

Corresponding Author:

Jyoti Neeli,
Department of Information Science and Engineering,
Global Academy of Technology,
Visvesvaraya Technological University (VTU),
Bengaluru, VTU, Belagavi, Karnataka, India.
Email: jyotirneeli@gmail.com

1. INTRODUCTION

Wireless Adhoc network is characterized by the lack of supportive infrastructure and consists of various communicating devices (also called peers) in a very dynamic manner. These self-organizing peers are capable of maintaining connectivity among them by sharing their wireless capabilities [1]. This characteristic assists the wireless communication device to establish connectivity among each other where the source node can forward the data packet to the destination node either directly or indirectly through intermediate relay node [2-3]. Due to this decentralized mechanism of communication establishment and routing, there is less possibility of the availing key distribution center in the ad-hoc wireless network [4]. Neither it is feasible for availing a robust certificate authority because of which reason ad-hoc wireless network lacks precise identification of nodes [5]. Wireless Adhoc network is one suitable for the decentralized architecture deployment in the wireless network [6]. According to the theoretical study, it is believed that nodes in the ad-hoc wireless network always assume that any new node that joins its network has to follow the certain protocol of conduct. Unfortunately, this logic does not hold good in the majority of the practical communication system as there are various dynamic attacks in the ad-hoc wireless network evolving [7].

Owing to the decentralized scheme, there are various challenges associated with communication. Majority of the challenges are either associated with data forwarding/traffic related operation while other forms of problems are related to security problems in the ad-hoc wireless network [8-11]. At present, there are many security schemes evolved toward security applications of the ad-hoc wireless network [12-16], but very few approaches towards safeguarding the generalized architecture of the ad-hoc wireless network. It is because there are different types of applications in an ad-hoc wireless network with respect to the perspective of a communication protocol; therefore, the applicability of security solution of one application is never applicable to solve the same security problem in another application. For example, the same security solution cannot be offered towards securing blackhole attack in the mobile ad-hoc network and wireless sensor network as their routing management system is very different from each other. At the same time, another significant problem is that majority of the secure routing protocol is developed on the top of conventional routing protocol, e.g., adhoc on-demand distance vector (AODV), destination sequence distance vector (DSD), dynamic source routing (DSR, etc. Unfortunately, all these protocols already have challenges in its routing operation [17]. Therefore, without addressingsuch challenges, it is quite unwise and unpractical to use such protocols for securing the network. For example, AODV suffers from the problem of retaining stale routing information where the updates are less frequently carried out. The adversary can easily misuse such properties of routing problems by any means.

Various encryption-based schemes have been evolved up for secure routing scheme, but there are very less benchmarked studies in this regards. Hence, there is a need for such a security solution that offers a security solution based on the malicious behavior of the ad-hoc nodes, which works on the arena of all applications in the ad-hoc wireless network. Therefore, the proposed system introduces a simplified analytical model that is meant for taking a dynamic decision based on current local and global trust in order to assess the intention of the nodes present in the network. The current work also presents probabilistic modeling towards assessing various critical situations of the threats.

There are various approaches witnessed in the existing system towards addressing the security problems in the ad-hoc wireless network [18]. This section, the approaches associated with the malicious behavior of the node is reviewed. The work of Sharma et al. [19] has presented an authentication protocol for its neighboring nodes for resisting blackhole attack in the ad-hoc wireless environment. It has also been seen that frequently used routing schemes, e.g., adhoc on-demand distance vector (AODV) has been modified to offer dual acknowledgment scheme for authentication. Study towards incorporating bio-inspired algorithm has been seen in the work of Chintalapalli and Ananthula [20], which is about the selection of the secure routes in the mobile ad-hoc network. Considerations of the behavioural semantics, Yadav, and Gaur [21] have presented a framework that is developed based on the algebraic concept for secure data communication in the mobile ad-hoc network. A unique study carried out on Zheng et al., [22] has introduced a strategic mechanism using a hybrid duplex receiver. This logic confuses the malicious node to perform eavesdropping followed by forwarding as well as jamming the adversary signal.

Ali and Prasad [23]. The work of Girnar and Kaur [24] have studied the security of the ad-hoc network with respect to a neural network where the simulated outcome shows that the proposed system is resistive of blackhole attack and wormhole attack. The study towards enhanced data forwarding scheme presented by Kaurav and Joshi [25] is shown to offer resistance from eavesdropping attack to prove that the presented scheme offers better throughput, overhead, and data delivery performance. Adoption of a reinforcement learning scheme has been witnessed in the work of Mayadunna et al., [26] where a secure routing scheme has been developed using trust factor thereby contributed towards malicious node identification. Prevention mechanism towards conflicting behavior was discussed by Samreen and Jabbar [27] where an elimination strategy of the malicious node is developed based on the trust factor. Analysis of security strength of conventional ad-hoc routing scheme is carried out by Shabut et al., [28] where the technique is claimed of better performance on detection of eavesdropping attack mainly.

The existing system has also noticed the usage of classifier-based approach towards detection of the adversary in the ad-hoc network. The work of Shams and Rizaner [29] have used support vector machine to show that it can resist potential attacks with better data forwarding performance. Usage of trust management has been seen in the study of Guo et al. [30] where an integrated approach of fuzzy logic as well as information quantification concept for resisting potential attacks in the ad-hoc wireless network. The work of Trivedi et al. [31] has used reputation-based modeling towards the identification of intrusion in the presence of mobility in the ad-hoc network environment. The work presented by Patwardhan et al. [32] has used encryption and key-based management towards strengthening the authentication process. Apart from this, the other approaches are predictive (Sowah et al., [33]), modified AODV based (Zant et al., [34]), study-based (Chandan et al. [35]), routing-based (Vadavi et al., [36]) and signal strength-based (Faisal et al., [37]). Abdullah et al., [38] have illustrated data gathering algorithm for wireless sensor networks by using joint mobile aspects.

Bhatia and Tomar [39] have presented bandwidth optimization and power efficient dynamic source routing protocol in MANETs. Jyoti Neeli et al., [40] have presented various approaches undertaken by existing literature to a discrete security issue and also examine the effectiveness point of the security. The research study was done by Tuberquia and Hernandez [41] a novel approach in cognitive radios by using an algorithm called evolutionary. The work of This study mainly focuses on reconfigurable fault tolerant on chip architectur with hierarchical agent based monitoring system for enhancing the performance of network based multiprocessor system on chip against faulty links and nodes. Jati et al., [42] this works mainly focuse on classification methods to enhance the security technique based on the humn gaint. The GAIT is one ofthe biometric techniques that might be employed to recognize the person. The next section briefs of problems that are targeted to be addressed in the proposed system.

Existing system towards securing the routing mechanism in the ad-hoc wireless network is more or less symptomatic where the prime inclination of the presented approaches are focused on offering security solution towards specific attacks. After reviewing the work carried out towards the secure communication in the ad-hoc wireless network, it was seen that majority of the work carried out is towards addressing particular security breach which loses its applicability towards resisting other forms of attacks. It is because every attack has different strategies, but the mode of initiating the attacks are more or less the same. If the malicious behavior of the node cannot be accurately confirmed, then offering protective measures will be quite a difficult task. Another essential review finding is that there are very less journals representing security problems in the ad-hoc wireless network and there is a number of research on specific applications, e.g., mobile ad-hoc network, vehicular network, sensor network, etc. Irrespective of all of these fall under the domain of ad-hoc network, but their routing mechanism vary from each other. It shows that secure routing scheme of sensor network has lesser applicability on the mobile ad-hoc network and vice-versa. Hence, a generalized scheme is required. There are few studies where attack resistivity strategy is developed based on generalizing or complex malicious behavior. Therefore, the research problem is "Developing a resistivity against maximum attack using cost-effective modeling approach in the ad-hoc wireless network using the unique features of malicious behavior”.

The proposed study consider analytical research methodology in order to investigate the behavior of the lethal attacks in the ad-hoc wireless network as well as develop a strategy for resisting the spread of such intrusion further. The block diagram of the proposed system is shown in Figure 1. The block diagram exhibits the scheme towards the identification and prevention of variants of attacks on the ad-hoc wireless network. The proposed model develop an adversarial model using three different, which is about observing the malicious behavior of the destination/intermediate node in the neighborhood.

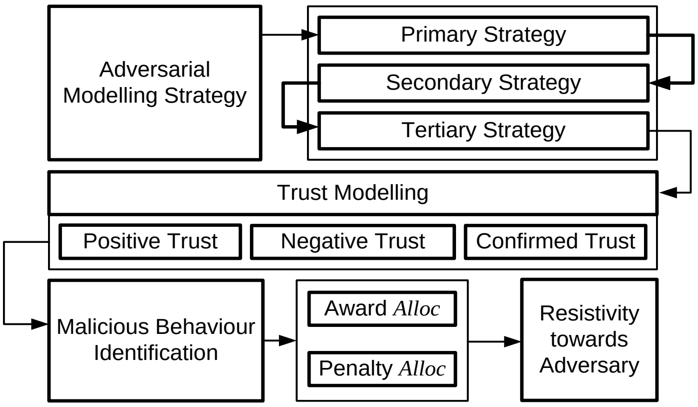

Figure 1. Block diagram of proposed methodology

The complete observation is carried out based on trust management, where trust is calculated using the probability concept. The final stage of the study implementation is about identifying the malicious, which is further followed by either continuing the communication or stopping the communication using the allocation of the award/penalty. The formulation of the award and penalty is developed based on various extrinsic factors, e.g., amount of resources utilized in undertaking a specific task, profit obtained by undertaking a specific task, the penalty for false alarm (for regular node), etc. These parameters are developed in such a manner that computation of them will always give an outcome in the range of 0 and 1. This is carried out to use the scope of statistical inferencing system for the numerical outcome obtained. The prime contribution of the proposed system is that it implements a unique adversarial model which not only increases the applicability of the proposed system but also introduces a scheme to resist such lethal threats. The next section discusses the algorithm design.

2. ALGORITHM IMPLEMENTATION

The development of the complete algorithm is carried out based on the observation towards the secured trust computation by the source node towards the intermediate node selected for forwarding the data packet. The mechanism of confirming the node to be communicated with is an attacker, or regular node depends upon novel analytical modeling of the three test environment as follows:

a. Test-Environment-1: In this test environment, the model will consider that both attacker and the regular node will adopt an action that offers than maximum award towards their motive. It means that regular node will be awarded maximum when they choose to capture the attacker while the attacker node will get the maximum award when they can successfully launch the attack. This test environment is opted for challenging modeling of a dynamic attack scenario.

b. Test-Environment-2: In this test environment, the action adopted by the next node is unknown and cannot be predicted by the other node. It also ensures that action adopted by a specific node is selected with a hidden agenda of obtaining the maximum award. The difference in all the test environments are: In the 1st test environment, once a node executes its actions then the action of next node is somewhat predictable and defined, which is different in the 2nd test environment.

c. Test-Environment-3: In this test environment, the information associated with the execution of the actions of either of the nodes is completely unknown or impartial. It offers a balance between both the regular node and attacker in terms of obtaining more awards. The difference between the 1st-2nd test environment and 3rd test environment is that the information is quite complete in 1st-2nd test environment while 3rd test environment does not have any form of the definition of attack. This makes the 3rd test environment more lethal and appropriate to assess the identification of different forms of attacks.

Apart from the test-environment mentioned above, the proposed study defines the term action as a specific task carried out by nodes. For clarity in implementation, the proposed model considers that there are two sets of actions viz. A_{comm} and A_{dist}. It means that there are a certain common set of actions A_{comm} between regular and attacker node while there is a specific set of action A_{dist}, which is highly unique and different from each other. It will also mean that an attacker node will not easily execute A_{dist} as the probability of them being caught will be high. So, an attacker will attempt execution of A_{comm} in order to gain the trust of a regular node. Hence, there are various complex scenarios artificially and analytically developed in order to develop a secure routing scheme. The first algorithm is designed for identification of the attacker node, and its steps of execution are as follow:

```
Algorithm for Identification of Attacker Node
Input: n (number of nodes), C (Cut-off)
Output: identification of the attacker node
Start
1. while $H_1<C$ Do
2.        If $H_2 \leq G$ then
3.          Choose M(prob→1)
4.       Else
5.          Choose M(prob→x)
6.         End
7.       re-compute $P_1$, $P_2$, $H_2$, and $P_4$
8. End
9.  Flag i node as the attacker
End
```

The algorithm initially checks for a condition H_1 to be lesser compared with the cut-off value *C* (Line-1). The computation of H1 is carried out by obtaining the product of two significant information viz. i) probability of intrusion and ii) complete information of probability (i.e., certainty). The next step of the algorithm is to check if H_2 is lesser than the empirical value of G (Line-2). Here, H_2 can be defined as the probability of intrusion while the empirical variable G depends upon various external parameters, e.g., the profit received by a node after assisting it to forward a data, resources deployed by a node after assisting in forwarding data, and profit obtained after launching an attack. The variable G can also be defined as a probability of maximal profit during the intrusion. In such a case, the algorithm chooses M as a set of action representing forwarding of the data packet with maximum probability (Line-3); otherwise, it computes a new probability (Line-5). Finally, the algorithm updates the probability score, i.e., P_1 (Probability of regular node), P_2 (probability of data dropping), and H_2 (Probability of intrusion) and P_4 (Probability of incomplete information) (Line-7). All this computation is carried out by the source node for its immediate neighbor node and based on this probability computation; the algorithm makes a decision of flagging the node to be a malicious node. After the identification of the node is over, the next task is to offer preventive measure against the malicious node. The algorithm responsible for preventing the node from further intruding is as follows:

```
Algorithm for prevention of attacker node
Input: i (node), A (Award), P (Penalty)
Output: isolation of i
Start
1. If i=attacker
2.    If $i \rightarrow j$
3.      Allocate $A^{-}$
4.   Else
5.      Allocate $P^{++}$
6.      update all neighboring nodes & isolate i;
7.  End
End
```

The above algorithm is responsible for resisting the further spread of the attack. This algorithm becomes functional only after the identification of the i^{th} node as an attacker node from the prior algorithm (Line-1). Different from any existing intrusion prevention approach, the proposed system doesn't directly stop the malicious node, but rather, it checks the intention of the malicious node. If the probability calculation carried out by the regular source node, suggest that a malicious node is assisting in forwarding the data packet than it is allowed to do so. Interestingly, once the regular node has identified that the other node is malicious (Line-1) and has a harmful intention, it calculates the probability of attack. If the probability of an attack is very low (irrespective of being a malicious node), it is permitted to forward the data packet. However, while doing so, the malicious obtained a reduced amount of award (Line-3) from the source node. Hence, this mechanism optimizes even the malicious node in a highly controlled environment to assist in data packet forwarding. Moreover, better control over the vulnerable situation is made by allocating the only reduced value of incentive as an award; otherwise, they are allocated with penalty value (Line-5). On the other side, the algorithm also checks for if there was any form of error in flagging the other node as a malicious node. In order to avoid any form of false positive in flagging the other node as the malicious node, the regular node double check the local as well as a global trust factor for the targeted node from all the neighboring node of the targeted node. It is because as per the test-environment-1, the regular node should get the highest award if they can positively capture the attacker node; however, this might be challenging due to test environment-2 and test environment-3. In such a case, the attack information will be vague and improper, and there are probabilities of error in flagging correctly. Hence, in such case, the regular node is also penalized if they make a mistake of flagging a wrong node into malicious.

The complete idea of the prevention technique adopted in the proposed system is as follows: Whenever a node makes any decision of undertaking a task (it could be related to forwarding beacon/data, rejecting forwarding data, raising an alarm of malicious node, launching an attack, etc.), there is an incentive allocation for it. This incentive is allocated in the form of award and penalty. Hence, based on the 1st test environment, both regular, as well as the malicious node, will try to be dominant with each other; however malicious node does so with the caution of not getting caught if the incompleteness about the trust factor is spontaneously found to be increasing with increase of simulation than it is a better scenario to tell that the node is malicious node. Interestingly, direct detection of the malicious node makes the malicious node much more aware of the surveillance system; hence, the algorithm covertly computes and confirm about the illegitimacy of the node and harness them to highest extent to forward data packet. In such case, if the malicious node assists in forwarding data, their motive of presence in the network never fulfills, and instead, they will be just drained of their resources only for assisting in data forwarding. The moment the probability computation predicts that a specific malicious node could launch an attack in its next task execution, they are offered with the penalty. Once the malicious node is isolated, the routing is continued, and information about the successfully established routing path is given more weightage, and all intermediate node involves get increased trust value. This principle of secure routing by identifying malicious behavior applies to any form of adversaries in the ad-hoc wireless network. It is because irrespective of any specific characteristics of the adversary, all malicious nodes initially mimic the regular node to gain trust and then initiate attack after suitably finding an appropriate time. The next section of the paper discusses the results obtained after implementing the proposed logic.

3. RESULTS ANALYSIS

The prime strategy of the proposed analysis is to assess the performance of the identification of the malicious node as well as trace out the respective performance of the data forwarding features. A secure routing protocol can be only said to be robust it is capable of maintaining a good balance between the security as well as the data forwarding performance. The scripting of the proposed logic was carried out in MATLAB over the normal 64-bit windows platform. The simulation environment consists of 200 mobile nodes combining both regular and malicious nodes with no direct input of node identity for malicious node prior to simulation. The assessment is carried out with respect to throughput, routing overhead, latency, and processing time. A comparative analysis is carried out with respect to SEAD [43] and SRP [44] protocol, which is also secured routing schemes in the ad-hoc wireless network.

The graphical outcome shows that the proposed system offers better throughput see Figure 2 and lower routing overhead see Figure 3 compared to existing SRP and SEAD protocol. The prime reason behind the throughput improvement is that the proposed system offers better formulations of routes in faster track as it has frequent updates about the global trust values. Moreover, the adoption of probability based modeling further boosts up the process of exploring and confirming the secured path.

The outcome shown in Figure 4 exhibits that there is a considerably lower routing overhead. A closer look into Figures 2-4 shows that increase of malicious nodes in terms of percentile doesn't offer many challenges to communication performance. As the mobile nodes access their routing table from their shared memory, hence, obtaining global trust factor is quite faster. Moreover, the proposed system offers faster processing time see Figure 5 as it has no inclusion of any iterative operation, e.g., encryption as well as it doesn't have any dependency of storing any secret keys as authentication is always done when demanded. Therefore, the proposed system can be said to offer better security options cost-effectively.

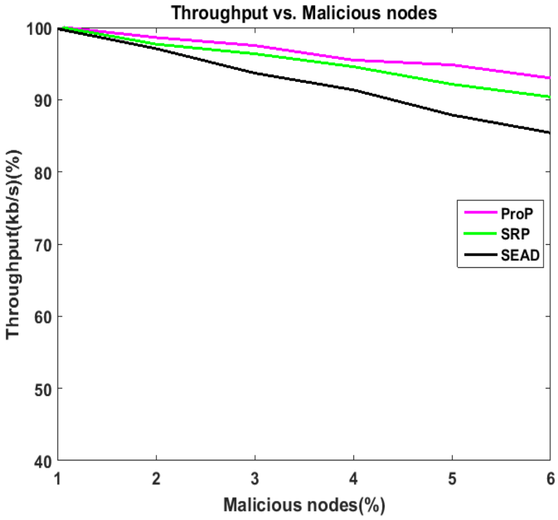

Figure 2. Comparative analysis of throughput

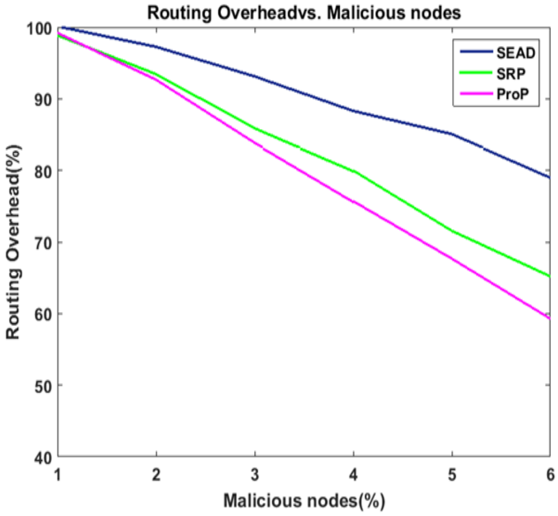

Figure 3. Comparative analysis of routing overhead

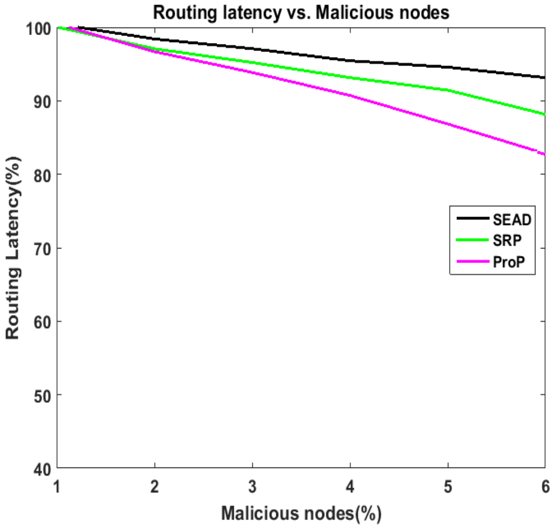

Figure 4. Comparative analysis of routing latency

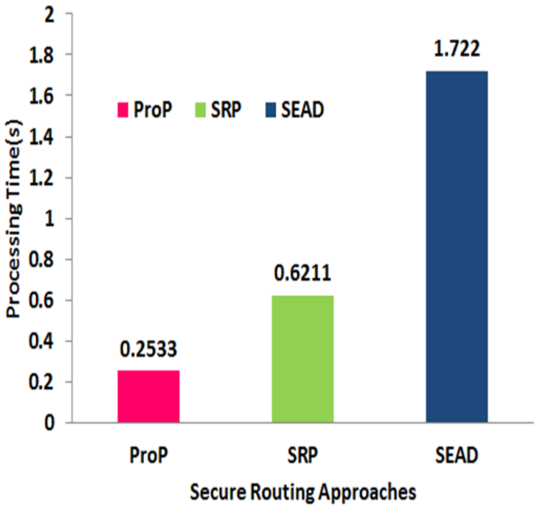

Figure 5. Comparative analysis of processing time

4. CONCLUSION

Security breach and vulnerability has always been a significant threat to the ad-hoc wireless network owing to the lack of centralized architecture. Existing approaches are quite specific to the forms of the threats, and hence, they are slightly non-practical when the application of the ad-hoc wireless network is exposed to the different adversary. Hence, the proposed system addresses this problem by developing a probability model that is capable of identifying the malicious behavior of node and hence is effective against the maximum number of attacks. The contribution of the proposed study are as follows: i) without any usage of encryption, the proposed system is capable of identifying and resisting the threat, ii) a successful implementation of an attacker module under three challenging test environment is carried out to show enhanced scope and applicability, iii) it also offers faster updated of non-stale information unlike the conventional secured routing approaches, and iv) proposed system offers better data forwarding performance in contrast to existing security scheme.

REFERENCES

[1] H. Sedjelmaci, et al., “Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: A Bayesian game-theoretic methodology,” in *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 5, pp. 1143-1153, May 2017.

[2] L. Pycroft and T. Z. Aziz, “Security of implantable medical devices with wireless connections: The dangers of cyber-attacks,” in *Expert Review of Medical Devices*, vol. 15, no. 6, pp. 403-406, 2018.

[3] X. Geng, et al., “Defending wireless infrastructure against the challenge of DDoS attacks,” *Mobile Networks and Applications*, vol. 7, no. 3, pp. 213-223, 2002.

[4] H. Deng, et al., “Threshold and identity-based key management and authentication for wireless ad hoc networks,” in *International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004*, vol. 1, pp. 107-111, 2004.

[5] S. Yi and R. Kravets, “MOCA: Mobile certificate authority for wireless ad hoc networks,” *IDEALS*, 2004.

[6] H. F. Rashvand and H. C. Chao, “Dynamic Ad Hoc Networks,” *The Institution of Engineering and Technology*, pp. 447, 2013.

[7] S. Kurosawa, et al., “Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method,” *International Journal of Network Security*, vol. 5, no. 3 pp. 338-346, 2007.

[8] S. Sharmila and T. Shanthi, “A survey on wireless ad hoc network: Issues and implementation,” *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, Pudukkottai, pp. 1-6, 2016.

[9] S. Meguerdichian, et al., “Coverage problems in wireless ad-hoc sensor networks,” *Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No.01CH37213)*, Anchorage, AK, USA, vol. 3, pp. 1380-1387, 2001.

[10] V. Ramasamy, “Recent advances in ad-hoc networks,” *2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, pp. 132-132, 2017.

[11] A. Vij and V. Sharma, “Security issues in mobile adhoc network: A survey paper,” *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Noida, pp. 561-566, 2016.

[12] M. S. Athulya and V. S. Sheeba, “Security in Mobile Ad-Hoc Networks,” *2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12)*, Coimbatore, pp. 1-5, 2012.

[13] R. K. Singh and P. Nand, “Literature review of routing attacks in MANET,” *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Noida, pp. 525-530, 2016.

[14] Margi, Cíntia B., Marcos A. Simplicio Jr, Mats Naslund, Bruno T. de Oliveira, Paulo SLM Barreto, Richard Gold, Gustavo T. de Sousa, and Tereza CMB Carvalho, “Impact of operating systems on wireless sensor networks (security) applications and testbeds,” In *2010 Proceedings of 19th International Conference on Computer Communications and Networks*, IEEE, pp. 1-6, 2010.

[15] A. Kannammal and S. S. Roy, “Survey on secure routing in mobile ad hoc networks,” *2016 International Conference on Advances in Human Machine Interaction (HMI)*, Doddaballapur, pp. 1-7, 2016.

[16] V. S. Bhargavi, et al., “A hybrid secure routing scheme for MANETS,” *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS*), Pudukkottai, pp. 1-5, 2016.

[17] H. Yang, et al., “Security in mobile ad hoc networks: challenges and solutions,” in *IEEE Wireless Communications*, vol. 11, no. 1, pp. 38-47, 2004.

[18] J. Neeli and N. K. Cauvery, “Insight to research progress on secure routing in wireless Ad Hoc network,” *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, 2017.

[19] N. Sharma, et al., “Provisioning of Quality of Service in MANETs performance analysis & comparison (AODV and DSR),” *2010 2nd International Conference on Computer Engineering and Technology*, Chengdu, pp. V7-243-V7-248, 2010.

[20] R. M. Chintalapalli and V. R. Ananthula, “M-LionWhale: multi-objective optimisation model for secure routing in mobile ad-hoc network,” *IET Communications*, vol. 12, no. 12, pp. 1406-1415, 2018.

[21] P. Yadav and M. Gaur, “A behavioural theory for intrusion detection system in mobile ad-hoc networks,” in *Proceedings of the 2nd International Conference on High Performance Compilation, Computing and Communications*, pp. 51-60, 2018.

[22] T. Zheng, et al., “Physical Layer Security in Wireless Ad Hoc Networks Under A Hybrid Full-/Half-Duplex Receiver Deployment Strategy,” in *IEEE Transactions on Wireless Communications*, vol. 16, no. 6, pp. 3827-3839, Jun. 2017.

[23] S. S. Ali and B. V. V. S. Prasad, “Secure and energy aware routing protocol (SEARP) based on trust-factor in Mobile Ad-Hoc networks,” *Journal of Statistics and Management Systems*, vol. 20, no. 4, pp. 543-551, 2017.

[24] N. Girnar and S. Kaur, “Intrusion detection for Adhoc networks in IOT,” *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, pp. 110-114, 2017.

[25] H. Kaurav and K. K. Joshi, “Improved routing security using intrusion detection system in mobile Ad Hoc network,” in *2017 International Conference on Trends in Electronics and Informatics (ICEI)*, Tirunelveli, pp. 172-176, 2017.

[26] H. Mayadunna, et al., “Improving trusted routing by identifying malicious nodes in a MANET using reinforcement learning,” *2017 Seventeenth International Conference on Advances in ICT for Emerging Regions (ICTer)*, Colombo, pp. 1-8, 2017.

[27] S. Samreen and M. A. Jabbar, “Countermeasures for Conflicting Behavior Attack in a Trust Management Framework for a Mobile Ad hoc Network,” *2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Coimbatore, pp. 1-4, 2017.

[28] A. M. Shabut, et al., “Malicious insider threats in tactical MANET: The performance analysis of DSR routing protocol,” *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, Dhaka, pp. 187-192, 2017.

[29] E. A. Shams and A. Rizaner, “A novel support vector machine based intrusion detection system for mobile ad hoc networks,” *Wireless Networks*, vol. 24, no. 5, pp. 1821-1829, 2018.

[30] J. Guo, et al., “A new trust management framework for detecting malicious and selfish behaviour for mobile ad hoc networks,” *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, Changsha, pp. 142-149, 2011.

[31] A. K. Trivedi, et al., “A semi-distributed reputation based intrusion detection system for mobile adhoc networks,” *arXiv:1006.1956*, 2010.

[32] S. H. Schneider, et al., “Assessing key vulnerabilities and the risk from climate change,”*Climate Change 2007: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change, Cambridge University Press, Cambridge, UK*, pp. 779-810, 2007.

[33] R. A. Sowah, et al., “Detection and Prevention of Man-in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in Artificial Neural Networks (ANN),” *Journal of Computer Networks and Communications*, vol. 2019, pp. 1-14, 2019.

[34] M. A. Zant and A. Yasin, “Avoiding and Isolating Flooding Attack by Enhancing AODV MANET Protocol (AIF_AODV),”*Security and Communication Networks*, vol. 2019, pp. 1-12, 2019.

[35] R. R. Chandan and P. K. Mishra, “A Review of Security Challenges in Ad-Hoc Network,” *International Journal of Applied Engineering Research*, vol. 13, no. 22, pp. 16117-16126, 2018.

[36] J. V. Vadavi and A. G. Sugavi, “Detection of black hole attack in enhanced aodv protocol,” *2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN)*, Gurgaon, pp. 118-123, 2017.

[37] M. Faisal, et al., “Identity attack detection system for 802.11-based ad hoc networks,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, pp. 128-144, 2018.

[38] A. Abdullah, et al., “Data collection algorithm for wireless sensor networks using collaborative mobile elements,” *International Journal of Electronical and Computer Engineering (IJECE)*, vol. 9, no. 3, pp.2131-3140, 2019.

[39] B. Bhatia, et al., “Extended Bandwidth Optimized and Energy Efficient Dynamic Source Routing Protocol in Mobile Ad-hoc Networks,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 3, pp. 1460-1466, 2018.

[40] J. Neeli and N. K. Cauvery, “Framework for Capturing the Intruders in Wireless Adhoc Network Using Zombie Node,” in *Computer Science On-line Conference*, vol. 765, pp. 346-355, 2018.

[41] M. Tuberquia and C. Hernandez, “New Approaches in Cognitive Radios using Evolutionary Algorithms,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 3, pp. 1636-1646, 2018.

[42] A. N. Jati, et al., “Comparison Analysis of Gait Classification for Human Motion Identification Using Embedded Computer,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 6, pp. 5014-5020, 2018.

[43] Y.C. Hu, et al., “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,” *Proceedings Fourth IEEE Workshop on Mobile Computing Systems and Applications*, Callicoon, NY, USA, pp. 3-13, 2002.

[44] Z. Liu, et al., “Secure routing protocol based trust for ad hoc networks,” *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)*, Qingdao, pp. 279-283, 2007.

BIOGRAPHIES OF AUTHORS

Jyoti Neeli, is currently a research scholar in RVCE working as an Associate professor in Department of Information science & Engineering Global Academy of Technology Bengaluru. She has completed M .Tech in Computer Science & Engineering from VTU. She has a total experience of 17years in teaching and 6 years in R &D. Her area of interest includes Computer networks, Software testing, Mathematical models.

Dr. N. K. Cauvery, is Professor in Department of Informaton science & Engineering, R V College of Engineering, Bengaluru. She has completed Ph. D from VTU with research title as “Routing in Computer Network using Genetic Algorithm”. She has total experience of 20 years in teaching and 7 years in R&D. Her publications includes papers both in national and international conferences and journals. Her area of interest includes Computer network, Compiler Design, Genetic Algorithm