Probabilistic Framework for Assessing the Threat Level using Novel Decision Constructs in Mobile Adhoc Network

V. Sangeetha[1] and S. Swapna Kumar[2]

(Corresponding author: V. Sangeetha)

Department of Computer Science and Engineering, Kammavari Sangha Institute of Technology[1]
14, Kanakapura Main Road, Municipal Corporation Layout, Raghuvanahalli, Bengaluru, Karnataka 560062, India
(Email: sangeethares13@gmail.com)
Department of Electronics and Communication Engineering, Vidya Academy of Science and Technology[2]
P.O. Thalakottukara, Kaipparambu, Thrissur, Kerala 680501, India

(Received June 19, 2017; revised and accepted Nov. 5, 2017)

Abstract

The existing secure routing protocol in Mobile Adhoc Network (MANET) lacks the capability of identifying the dubious communication behavior of a mobile node, which is essential in order to construct policy to resist them. This could happen when the malicious nodes choose to act like a regular node in order to bypass security. After reviewing the existing research approach, we found that existing studies are carried out in highly controlled research environment which is no more applicable if the environment changes. Therefore, we introduce a framework which is capable of assessing the level of legitimacy of the node in a network before confirming the route establishment with it. The study uses a novel decision making constructs for implementing its strategy of communication and it also incorporates strategic construction of assessing the security threat. The study outcome of proposed system is found to excel better communication performance when compared with existing security routing protocols in MANET.

Keywords: Intrusion Detection; Intrusion Prevention; Malicious; Mobile Adhoc Network

1 Introduction

Mobile Adhoc Network is one of the best way to provide seamless communication platform without any kind of fixed infrastructure. Hence, this communication feature allows it to perform adhoc based communication [9, 22]. Significant advantage of MANET system includes

1) Infrastructure independent;
2) Multi-hop routing;
3) Autonomous terminal;
4) Dynamic topology;
5) Fault tolerance;
6) Cost effective [1, 7].

It has its wide range of applicability in tactical network, emergency services, education applications, location-based services [12, 19, 20]. However, an interesting fact to observe that although MANET is being studied and investigated from more than two decades, but still date there are few application that is commercially available or known to the common people.

The communication in MANET is supported by three different routing protocols *i.e.* proactive, reactive, and hybrid [18]. At present, there are more than thousand numbers of research work on routing protocols till date, but majority of them suffers from one or other issues. For an example, proactive protocols suffers from slow convergence rate, tendency for loop creation, higher dependencies on resources, unexploited routing information *etc.* Reactive protocols suffers from out-date routing information, maximized delay, overhead cost, *etc.* Finally, hybrid protocol suffers from usage of random schemes (proactive) over the simulation area, latencies involved in inter-zones routing, routing over zones are highly resource dependent. Hence, it will be unwise to highlight any specific routing protocol in MANET to be highly efficient one. Although, these routing protocols are sufficient to form communication among mobile nodes but they are not enough powered to resist different forms of attacks *e.g.* active attack and passive attack in MANET. Some of the attacks in MANET are modification, Denial-of-Service, Spoofing, Impersonating, Masquerade, wormhole attack, Sybil attack, black-hole attack, rushing attack, replay attack, *etc.*

Some of the standard routing protocols in MANET are

1) Secured Efficient Distance vector (SEAD);
2) Secured Destination Sequence Distance Vector

(SDSDV);

3) Secure Line State routing protocol (SLSP);
4) Server Routing Protocol (SRP);
5) Byzantine Failure Resilient Protocol;
6) Authenticated Routing for Adhoc Networks (ARAN);
7) Secured Position-Aided Adhoc Routing (SPAAR);
8) Security Aware Routing (SAR), *etc.* [24, 28, 31].

However, all the existing secure routing protocols suffer from problems that really don't assist in proper identification [11].

At present there are also various techniques based on trust and reputation [27] meant for checking the security validity of the next node. Unfortunately, all these techniques have not offered any evidence that their outcome in the form of identification process is reliable or not. Hence, existing process doesn't offer any form of standardized validity that the outcome generated by security protocol should be believed as universal standard. This is a serious problem as it doesn't lead us to find the distinct difference between different types of mobile nodes in MANET. Therefore, if there is any malicious node pretending to be normal node existing within simulation that it may lead to collateral damage. Therefore, the proposed system offers a framework that applies the potential of decision making approach for strategy building in order to investigate the pattern of malicious communication behavior of mobile nodes.

The outcome of the study is meant to be used for both intrusion detection system as well as intrusion prevention system. The study uses multiple parameters of probability to find the level of authenticity of the mobile nodes present within the network. The proposed study is essentially meant for adopting a communication strategy based on the environmental condition. Section 1.1 discusses about the existing literatures where different techniques are discussed for secure routing protocols in MANET followed by discussion of research problems in Section 1.2 and proposed solution in Section 1.3. Section 2 discusses about algorithm implementation followed by discussion of result analysis in Section 3. Finally, the conclusive remarks are provided in Section 4.

2 Background

This section presents the brief highlights of the existing research-based approaches towards securing the communication in MANET. Cao *et al.* [3] have presented a framework that evaluates the capacity of the secrecy along with the delay factor in MANET using empirical-based approach. Anand *et al.* [2] introduced a scheme that investigates the misbehavior of the node using dynamic approach of partially retaining the malicious information. Matam and Tripathy [17] have presented a multi-cast routing using digital signature in order to resist wormhole attack. Although this work is targeted for mesh network but it is equally applicable for MANET. Surendran and Prakash [26] have used bio-inspired algorithm for retaining maximum resiliency of routing process in MANET. Zhang *et al.* [33] have presented a technique that can offer mitigation from jamming-based intrusion in MANET.

Study towards investigating traffic behavior was carried out by Qin *et al.* [21] using statistical approach. Liu and Yu [14] have introduced a routing technique that offers both robust authentication as well as anonymity in MANET using digital signature. Sekaran and Parasuraman [23] have used conventional cryptographic approach in order to secure the routing protocol. Usage of network code for supporting a cryptographic scheme is seen in the work of Zhang *et al.* [18] for enhancing the confidentiality. Shakshuki *et al.* [10] have presented a unique mechanism of intrusion detection system on the basis of the acknowledge in the control message.

Liu *et al.* [15] have enhanced the reliability by presenting a clustering scheme for assisting in revocation of certificate in MANET. Lv and Li [16] have implemented a mechanism for securing group-based communication system in MANET. Study towards trust effectiveness is emphasized by Zhao *et al.* [34] considering the patterns of cyclic movements using stochastic approach and Bellmam-Ford algorithm. Zhao *et al.* [35] have presented a mechanism for identifying the extent of risk involved in capturing the response message in MANET. Chen and Wu [4] have designed a secure protocol for safeguarding the anonymity process during routing using hash function.

El-Defrawy and Tsudik [6] have also focused on privacy preservation using group signature for resisting suspicious node to take part in routing process. Dhurandhar *et al.* [5] have implemented a scheme for incorporating robust security while routing among the networks of friendly nodes. Study towards optimal secrecy was carried out by Liang *et al.* [13] towards ensuring enhanced throughput in communication process. Xu *et al.* [29] have presented a technique that performs execution of trust from kernel level. Shen and Zhao [25] have also emphasized on incorporating a technique to maintain anonymity towards positional information during the routing process in MANET.

Hence, it can be seen that there are various techniques that has been evolved since last decade for securing the routing process in MANET. All the techniques play different level of roles to address security problems as well as all of them are implemented towards routing security itself. Each one of the protocol has its own advantages in form of security strength. The next section briefly discusses about the problems explored from the existing system.

3 Research Problem

The significant research problems are: Existing solutions are specific to the routing adversaries and its applicability on different environment is yet to be proven. Studies

towards identifying malicious behavior have not been assessed deeply in existing system that is not capable of differentiating the characteristics feature of nodes. Influence of increasing level of attack (be it any) towards communicational performance is not yet tested in existing system. Existing studies also doesn't assure the effectiveness / reliability of outcome of intrusion detection system in case of complex attack scenario.

Therefore, the problem statement of the proposed study can be stated as *"It is technically a difficult task to assess the level of legitimacy of the neighborhood node if the malicious node chooses to either act as normal node or self node in order to achieve their aim of intrusion".*

4 Proposed Solution

The prime purpose of the proposed work is to present a novel framework that uses the strategic approach for constructing decision thereby assisting the node to perform legitimacy evaluation for secured routing in MANET. The adopted scheme of proposed system where the significant contribution lies in behavioral modeling of a mobile node into malicious and normal node as shown (see Figure 1).

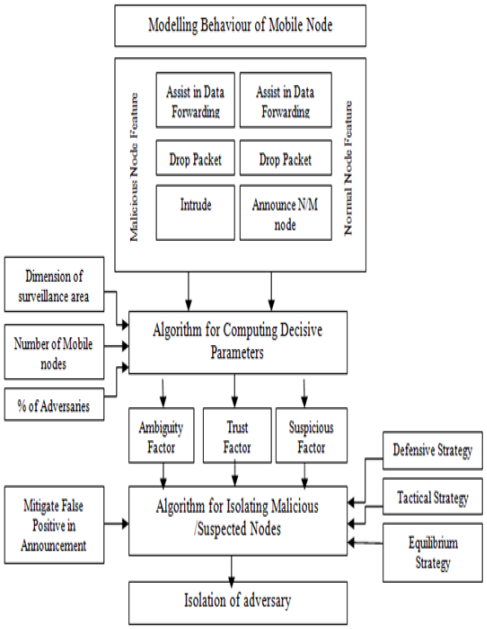

Figure 1: Adopted schema of proposed system

We formulate conditional feature stating that there are common and uncommon behavior for both the type of nodes. The common behavior is assisting the node in data forwarding and dropping packet. However, uncommon behavior is that actions of intrusion is only shown by adversary while announcing the node as malicious (M) or normal (N) is the feature of normal node.

The algorithm construction of proposed system takes the different form of inputs which after processing leads to evaluation of statistical information about ambiguity factor, trust factor, and suspicious factor using simple mathematical approach (discussed in the algorithm step in next section). The algorithm also considers using multiple form of strategies that either of the nodes could possibly consider for achieving their objectives. The possibility of false positive towards the announcement is also formulated in the proposed system. The notion is that for a given simulation scenario of unknown identities of node, the proposed system evaluates the communication behavior of the nodes and confirms a decision based on statistical evaluation. The decision is finally confirmed by filtering any form of false positive information in order to ensure proper isolation of malicious node from the further process of routing in MANET. The next section discusses about algorithm implementation of this concept.

5 Algorithm Implementation

The algorithm is mainly responsible for assessing the unpredictable behavior of the mobile nodes in MANET where it is assumed that confidentiality of any nodes is unknown. This assumption will mean that the proposed system does not have any kind of prior information about the legitimacy of the mobile nodes. The proposed system runs two different algorithms where one of them is responsible for computing the security attributes responsible for making decisions of legitimacy nodes and the other algorithm is responsible for isolating the malicious or suspected nodes to be participating in the routing process.

Algorithm for Computing Decisive Parameters

Input: s_a, n, a, b
Output: τ, T, S
Start
1. init s_a, n, a,b
2. [x . y]= s_a-(2*b).arb(n)
3. for i=1:n
4. τ = k .a_1.a_2
5. T=(1- τ).a.$(a+b)^{-1}$ and S=(1- τ).b.$(a+b)^{-1}$
6. end
End

The above mentioned algorithm is responsible for computing the decisive parameters for exploring the legitimacy of a node in MANET. The algorithm takes the input of s_a (dimension of surveillance area), n (number of mobile nodes), a (% of Adversaries), b (boundary of surveillance area) (Line-1), which after process yields the computed outcome of τ (Ambiguity factor), T (trust factor), S (Suspicious factor). A closer look into this formulation will show that the system just takes the input of proportion information of adversary node as input and it is never aware of any specific node to become adversary. The next part is to perform random distribution of the node according to Line-2, where the variable b represents boundary of node. For effective computation, the pro-

posed system uses probability theory for defining two different parameters a and b representing quantity of nodes assisting in data forwarding and occurrences of identified intrusion or packet drop respectively. It should be noted that process of packet drop is not only characteristic of malicious node but even a normal node can also drop the packet because of genuine technical reasons.

Hence, now the modeling imposes quite a challenging scenario to identify malicious or adversary node. In Line-4, the variable a_1 and a_1 will represents (a.b) and (a+b)2. (a+b+1) respectively that is used for computing ambiguity factor. The variable k represent network coefficient. Similarly, the empirical representation of computation of trust T and suspicious factor S is as shown in Line-5. This computation is an iterative process and is carried out by the transmitting node while choosing its neighborhood nodes by evaluating their legitimacy first. The next part of the algorithm will further assist the node to confirm its decision by taking necessary security measures.

Algorithm for Isolating Malicious/Suspected Nodes

Input: $\mu 1$, $\mu 2$, $\mu 3$
Output: isolation of adversary
Start
1. [n] = [$\mu 1$, $\mu 2$, $\mu 3$]
2. if $\lambda * (1\text{-}\tau) <$ Threshold
3. if $\lambda <$ h
4. return strategy $\rightarrow v_1$
5. else
6. return strategy $\rightarrow v_2$
7. end
8. end
9. Compute τ, T, S
10. $\Omega = s_i$ *((c- v_1)/φ)
11. Flag n (max(card(τ))) $\rightarrow$ adversary
End

The above algorithm confirms the level of threat for its monitored nodes and isolates them from participating in the routing process. The algorithm takes the input of three different strategies i.e. $\mu 1$ (Defensive Strategy), $\mu 2$ (Tactical Strategy), $\mu 3$ (Equilibrium Strategy), which after processing leads to isolation of adversaries (Line-1). By defensive strategy, it will mean that normal node will always assist in data forwarding while malicious node will always intrude. Hence, defensive strategy is the easier one that can be adopted by node straightly. Tactical strategy will mean that malicious node may even forward data packet without harming anyone and normal node may drop the packet without having any intention of disrupting the ongoing communication. Therefore, the tactical strategy is the most challenging one where there are chances of misidentification of legitimacy of either of the nodes. However, we believed that a malicious node will never continue to forward a data packet for a longer duration of time as it may significantly drain their resources which will lower the success rate of their execution of harmful intention. Hence, at certain point of time, it will definitely intrude.

In order to solve this problem, the proposed system introduces a probability parameter λ that represents the probability that the identified mobile node is possibly an adversary. A statistical threshold is used which is compared with the probability of confirming that a node is malicious ($\lambda * (1 - \tau)$) (Line-2). A new temporary parameter h is used for computing the gain obtained by a mobile node for forwarding a data packet (Line-4). It should be noted that if the malicious node is forwarding the data packet that it will not have gain as it is only meant for initiating attacks. Similarly, if the regular node forwards data then its gain will increase. Therefore, the condition stated in Line3-Line7 is that, if the threat probability parameter λ is found to be minimal to h than it is only the possibility that a data forwarding event v_1 is taking place (Line-4) otherwise it will mean that data packet is dropped (Line-6). Although, this condition gives information about the state of data packet forwarding or dropping, but it doesnt give much clarity that if this information obtained from the node is normal node or malicious node. Hence, the decision cannot be confirmed although the nature of communication being regular or threatful is confirmed.

The solution to this problem is consideration of the third strategy called as $\mu 3$ (Equilibrium Strategy) that is also one of the possible characteristics of any node (Line-1). According to this characteristics, it will mean that a malicious node will obtain maximum gain if it achieves its intention of intrusion/attack as faster as possible without much resource consumption. Similarly, equilibrium strategy also states that a normal node has all the right to compute the legitimacy of its neighbor node and can declare them to be normal or malicious nodes depending upon the level of threats in communication as seen till Line-6.

Hence, we formulate a condition that if the normal node flags incorrect information about its neighborhood node than its gain value will reduce. Interestingly, we don't model any such characteristics of computing legitimacy for the adversary. It is because we believed that performing such computation is completely unnecessary for the adversary node as it will only result in draining its own resources, which should be used only for invoking attacks. After this, the algorithm recomputes the value of trust factor T, suspicious factor S, and ambiguity factor τ (Line-9). We define a parameter τ which is representation of false positive information about the neighborhood node computed by a normal node (Line-10). The variable s represents selected strategy of action by the node (Line-10) whereas the variable c represents computation of the probability of the threat level to higher intensity. The variable Ω represents probability of identifying a mobile node to be malicious, which will mean that higher value of Ω will provoke the normal mobile node to confirm that the identified mobile node is malicious node. At the same

time, the malicious node will ensure that it doesn't take such step so that value of Ω for itself comes to be higher as per the principle of equilibrium strategy.

Therefore, according to the equilibrium strategy, a regular node will be be continuing more number of packet dropping event as in that case its gain obtained will be exponentially reduced which will affect its i) trust value and ii) its resources too. At the same time, a malicious node will only keep on forwarding data as long as their gain of invoking an attack is more than the resource expenditure inorder to carry out an attack. Hence, it is eventual that an attacker node will not continue to be in the mode of forwarding the data packet as in that way it will minimize its gain, which is only meant for attack purpose. Therefore, an indication of the attack scenario is that consistent frequencies of packet dropping by a same node is a direct indication of the malicious node (Line-11).

Even if such characteristics is carried out by a normal node than we assume that involvement of such node is highly detrimental for routing performance and therefore, we choose to remove the identity of the compromised / malicious node from the routing table. Also, we find that there is a strong relationship between the ambiguity factor and Ω whereas we find that if the first one increases than the later one also increases. Hence, the cardinality of the ambiguity factor is consistently assessed. Our observation says that a normal node will never exhibit more occurrences of relayed information more close to ambiguity factor, which is the definite identification of the malicious node. Therefore, the proposed system can successfully offer better behavioral analysis of the mobile nodes and performs secure routing only after ascertaining that its link with neighborhood nodes are stable and not yet compromised. The algorithm incorporates more decision making capabilities to the mobile node by using three different strategies to select from. The next section discusses about the result being accomplished after implementing the proposed algorithm.

6 Result Analysis

The implementation of the algorithm discussed in prior section has been designed by MATLAB considering simulation area of $1200 * 1500m^2$. The analysis was carried out considering 100 mobile nodes where 10% of the nodes are considered to be an adversary. The proportion of adversaries can be varied to understand the impact. The implementation is also analyzed considering all the three different forms of strategies (defensive, tactical, and equilibrium). For better assessment of the study outcome, we consider comparative performance analysis with the most standard secured protocol in MANET i.e. Secured AODV [30] and ARIADNE [8].

As shown (see Figure 2) the proposed system offers better throughput performance as compared to that of existing system of SAODV and ARIADNE. The prime reasons behind this are many. One of the advantages of

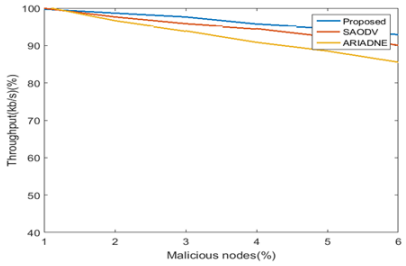

Figure 2: Comparative analysis of throughput

SAODV is its capability to detect and prevent misbehavior of node and it does so by using digital signature. Usage of digital signature offers significant resistance to the entry towards falsifying the legitimacy of the identity of the requester node. Although, SAODV schemes offers higher degree of resiliency towards authentication but it doesn't have capability to identify the selfish node like our system does. Therefore, if a regular node is found to drop packet for any good reason, SAODV still considers that node as malicious node. This causes the complete communication process to slow down causing lowering of the throughput with an increased level of authentication being demanded for with an increase in malicious node.

On the other hand, ARIADNE protocol is believed to offer resiliency against denial-of-service attacks in adhoc network, where the lightweights of the secured routing is confirmed by the usage of symmetric encryption. Usage of secret shares makes this protocol highly resistive towards authentication failures using digital signatures. ARIADNE also uses MAC protocol to perform robust authentication among each other. A closer look into both SAODV and ARIADNE protocol shows that it offers maximum resiliency when there is an attacker present in the network. However, none of these protocols are found capable of identifying any selfish node or compromised node, which is the main pitfall of existing system. Therefore, when SAODV and ARIADNE is allowed to be executed in our environment where the adversaries acts as a normal node and assists in forwarding data packet, both the protocol has failed to identify it.

Moreover, the existing protocol also found to be failing in understanding the motive that malicious node assist in data packet forwarding only because they want to increase trust level which lowers down the resource expenditure to greater degree. This causes the malicious node to meet an appropriate situation where it is not possible for any of the existing system to identify the degree of threat for the existing system. From the perspective of throughput as shown (see Figure 2), routing overhead as shown (see Figure 3), and routing latency as shown (see Figure 4), the trend is nearly similar. ARIADNE offers significant routing overhead along with increased delay because of its combined usage of MAC authentication with digital signature. Hence, existing on-demand routing schemes may offer good security against certain types of attacks but

doesn't excel optimal performance when it comes to communication performance in MANET where the identity of the attacker is not immediately disclosed.

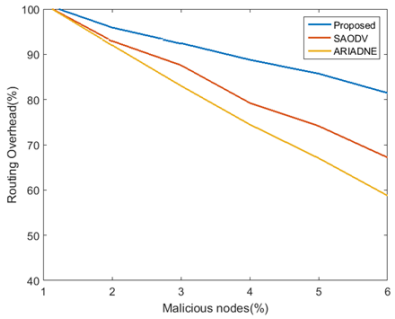

Figure 3: Comparative analysis of routing overhead

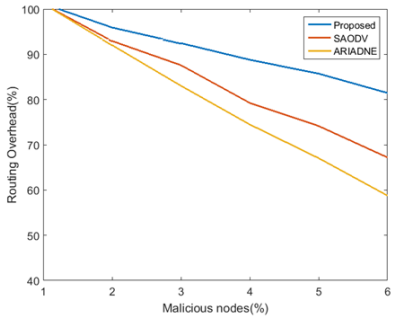

Figure 4: Comparative analysis of routing latency

Apart from this, we also find that proposed system takes approximately 0.31176 seconds in order to identify the malicious node while the existing system are found to consume 0.9762 seconds and 2.7669 seconds for SAODV and ARIADNE routing protocol tested on core i3 machine on windows platform. Moreover, the proposed system doesn't store any information during the run-time of the algorithm, all the information regarding the ambiguity factor, trust factor, suspicious factor are computed on run time. The advantage of this mechanism is that the system forcibly introduces lots of updated information about the legitimacy which assists the normal node to take a final decision with high true positive about the identity of the intruder by observing the communication behavior of them. The proposed system doesn't act directly as intrusion prevention system but rather it offers more insights on the typical behavior of a mobile node whose identity is suspected to be malicious. The framework is free from any form of encryption and therefore it is highly light weighted compared to any form of security protocol in existing system. The applicability of proposed framework is more on intrusion detection and prevention system for any form of malicious activity in MANET.

7 Conclusion

A robust and full proof security incorporation is one of the open-end challenging problems in MANET system primarily due to its effect of decentralization. The existing studies towards secure communication only offers resiliency from particular form of attack. This will mean that if the adversary launches two different form of attacks at same time than it is nearly impossible for the normal node even to identify the threat level and definitely will not possess enough time even to take a decision for adopting a precise mitigation. It may also be the case that mitigation policy doesn't even exists in the node being about to be victimized. Therefore, the proposed study presents such a technique that could compute the level of threat and takes necessary action in order to resist it. The outcome of the study was assessed to find that proposed system offers better throughput and minimal overhead and latency as compared to existing secured routing system in MANET.

References

[1] A. Abdullah, Al-khatib, W. A. Hammood, "Mobile malware and defending systems: Comparison study" *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 116-123, 2017.

[2] A. Anand, H. Aggarwal and R. Rani, "Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks," *Journal of Communications and Networks*, vol. 18, no. 6, pp. 938-947, 2016.

[3] X. Cao, J. Zhang, L. Fu, W. Wu and X. Wang, "Optimal secrecy capacity-delay tradeoff in large-scale mobile Ad Hoc networks," in *IEEE/ACM Transactions on Networking*, vol. 24, no. 2, PP. 1139-1152, 2016.

[4] S. Chen and M. Wu, "Anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks," *Journal of Systems Engineering and Electronics*, vol. 22, no. 3, pp. 519-527, June 2011.

[5] S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta and P. Dhurandher, "FACES: Friend-based Ad Hoc routing using challenges to establish security in MANETs systems," *IEEE Systems Journal*, vol. 5, no. 2, pp. 176-188, 2011.

[6] K. E. Defrawy and G. Tsudik, "ALARM: Anonymous location-aided routing in suspicious MANETs," *IEEE Transactions on Mobile Computing*, vol. 10, no. 9, pp. 1345-1358, 2011.

[7] B. S. Gouda, D. Patro and R. K. Shial, "Scenario-based performance evaluation of proactive, Reactive and hybrid routing protocols in MANET using random waypoint model," in *International Conference on Information Technology (ICoIT'14)*, pp. 47-52, 2014.

[8] Y. Hu, A. Perrig and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", *Wireless networks*, vol. 11, no. 2, pp. 21-38, 2005.

[9] A. Jamalipour, S. Kurosawa, H. Nakayama, N. Kato, Y. Nemoto, "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.

[10] P. Joshi, P. Nande, A. Pawar, P. Shinde and R. Umbare, "EAACK - A secure intrusion detection and prevention system for MANETs," in *International Conference on Pervasive Computing (ICPC'16)*, pp. 1-6, 2016.

[11] C. T. Li, M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks",*Information Sciences*, vol. 181, no. 23, pp. 5333–5347, Dec. 2011.

[12] C. T. Li, M. S. Hwang, C. Y. Liu, "An electronic voting protocol with deniable authentication for mobile Ad hoc networks," *Computer Communications*, vol. 31, no. 10, pp. 2534–2540, June 2008.

[13] Y. Liang, H. V. Poor and L. Ying, "Secrecy throughput of MANETs under passive and active attacks," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6692-6702, 2011.

[14] W. Liu and M. Yu, "AASR: Authenticated anonymous secure routing for MANETs in adversarial environments," in *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4585-4593, 2014.

[15] W. Liu, H. Nishiyama, N. Ansari, J. Yang and N. Kato, "Cluster-based certificate revocation with vindication capability for mobile Ad Hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 2, pp. 239-249, 2013.

[16] X. Lv and H. Li, "Secure group communication with both confidentiality and non-repudiation for mobile ad-hoc networks," *IET Information Security Technology*, vol. 7, no. 2, pp. 61-66, 2013.

[17] R. Matam and S. Tripathy, "Secure multicast routing algorithm for wireless mesh networks," *Journal of Computer Networks and Communications*, pp. 11-17, 2016.

[18] H. Moudni, M. Er-Rouidi, H. Mouncif and B. E. Hadadi, "Secure routing protocols for mobile ad hoc networks," in *International Conference on Information Technology for Organizations Development (ITOD'16)*, pp. 1-7, 2016.

[19] A. Negi, K. Ammayappan, V. N. Sastry, "A new secure route discovery protocol for MANETs to prevent hidden channel attacks," *International Journal of Network Security*, vol. 14, no. 3, pp. 121-141, 2012.

[20] A. A. Pirzada and C. McDonald, "Detecting and evading wormholes in mobile Ad-hoc wireless networks," *International Journal of Network Security*, vol. 3, no. 2, pp. 191-202, 2006.

[21] Y. Qin, D. Huang and B. Li, "STARS: A statistical traffic pattern discovery system for MANETs," in *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 2, pp. 181-192, 2014.

[22] A. Rana, D. Sharma, "Mobile ad-hoc clustering using inclusive particle swarm optimization algorithm," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 1-8, 2018.

[23] R. Sekaran and G.K. Parasuraman, "A secure 3-way routing protocols for intermittently connected mobile Ad Hoc networks," *The Scientific World Journal*, vol. 2014, pp. 13, 2014.

[24] P. K. Sharma and V. Sharma, "Survey on security issues in MANET: Wormhole detection and prevention," in *International Conference on Computing, Communication and Automation (ICCCA'16)*, pp. 637-640, 2016.

[25] H. Shen and L. Zhao, "ALERT: An anonymous location-based efficient routing protocol in MANETs," *IEEE Transactions on Mobile Computing*, vol. 12, no. 6, pp. 1079-1093, 2013.

[26] S. Surendran and S. Prakash, "An ACO look-ahead approach to QOS enabled fault - tolerant routing in MANETs," in *China Communications*, vol. 12, no. 8, pp. 93-110, 2015.

[27] Z. Ullah, M. H. Islam and A. A. Khan, "Issues with trust management and trust based secure routing in MANET," in *13th International Bhurban Conference on Applied Sciences and Technology (IBCAST'16)*, pp. 402-408, 2016.

[28] M. K. Verma, S. Joshi and N. V. Doohan, "A survey on: An analysis of secure routing of volatile nodes in MANET," in *CSI Sixth International Conference on Software Engineering (CONSEG'12)*, pp. 1-3, 2012.

[29] G. Xu, C. Borcea and L. Iftode, "A policy enforcing mechanism for trusted Ad Hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 3, pp.321-336, 2011.

[30] M. G. Zapata, "Secure Ad Hoc on-demand distance vector routing", *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 3, pp. 106-107, 2002.

[31] L. Zhang, X. Song, Y. Wu, *Theory, Methodology, Tools and Applications for Modeling and Simulation of Complex Systems*, Springer, 2016.

[32] P. Zhang, C. Lin, Y. Jiang, Y. Fan and X. Shen, "A lightweight encryption scheme for network-coded mobile Ad Hoc networks," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2211-2221, 2014.

[33] R. Zhang, J. Sun, Y. Zhang and X. Huang, "Jamming-resilient secure neighbor discovery in mobile Ad Hoc networks," in *IEEE Transactions on Wireless Communications*, vol. 14, no. 10, pp. 5588-5601, 2015.

[34] H. Zhao, X. Yang and X. Li, "cTrust: Trust management in cyclic mobile Ad Hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 6, pp. 2792-2806, 2013.

[35] Z. Zhao, H. Hu, G. J. Ahn and R. Wu, "Risk-aware mitigation for MANET routing attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 250-260, 2012.

Biography

V. Sangeetha is working as Associate Professor at Department of Computer Science and Engineering, K.S.Institute of Technology, Bengaluru, Karnataka, India. She received the B.E degree in Computer Science and Engineering from Acharya Institute of Technology, from Visvesvaraya Technological University (VTU), Bengaluru, Karnataka, India in 2004, and M.Tech in Computer Science and Engineering from R.V.College of Engineering, VTU, Bengaluru, Karnataka, India in 2011. Currently pursuing Ph.D in Computer Science & Engineering from VTU, Karnataka, India. Her current research interests include Network security, Wireless network, Embedded System. She has also a life membership of several professional bodies including Indian Society for Technical Education (ISTE); Institution of Engineers (IEI) and International Association of Engineers (IAENG).

S. Swapna Kumar, Ph.D., is Professor and Head, of Department of Electronics and Communication Engineering, in Vidya Academy of Science and Technology, Thrissur, Kerala, India. Presently, he is a Supervisor for the Ph.D. scholars under Visvesvaraya Technological University (VTU) and also an external examiner for Thesis evaluation/ Public Viva-voce of Ph.D. students. He has been in the teaching for profession courses under UG/PG level for nearly decade, and has worked for various national and international industries. He is a reviewer of several National and International journals. Besides, he has also authored a books on "A Guide to Wireless Sensor Networks" and "MATLAB easy way of learning". Dr. Swapna Kumar is a Fellow Member and Chartered Engineer of the Institution of Engineers (INDIA). He has also a life membership of several professional bodies, including Indian Society for Technical Education (ISTE) and IEEE. His area of interest include Networking, Security system, Fuzzy Logic, Data Communication, Electronics, Communication Systems, Embedded Systems, LaTeX, MATLAB modeling and simulation.