International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 2, April 2020, pp. 1552~1560
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i2.pp1552-1560

Novel framework using dynamic passphrase towards secure and energy-efficient communication in Manet

Chethan B. K.[1], M. Siddappa[2], Jayanna H. S. [3]
[1]Department of Information Secience and Engineering, Sri Siddhartha Institute of Technology, India
[2]Department of Computer Science and Engineering, Sri Siddhartha Institute of Technology, India
[3]Department of Information Secience and Engineering, Siddaganga Institute of Technology, India

Article Info

Article history:

Received Juni 6, 2019
Revised Oct 1, 2019
Accepted Oct 17, 2019

Keywords:

Encryption
Energy
Mobile adhoc network
Resource
Security

ABSTRACT

At Mobile Adhoc Network (MANET) has been long-researched topic in adhoc network owing to the associated advantages in its cost-effective application as well as consistent loophopes owing to its inherent charecteristics. This manuscript draws a relationship between the energy factor and security factor which has not been emphasized in any existing studies much. Review of existing security approaches shows that they are highly attack specific, uses complex encryption, and overlooks the involvement of energy factor in it. Therefore, the proposed system introduces a novel mechanism where security tokens and passphrases are utilized in order to offer better security. The proposed system also introduces the usage of an agent node which communications with mobile nodes using group-based communication system thereby ensuring reduced computational effort of mobile nodes towards establishing secured communication. The outcome shows proposed system offers better outcome in contrast to existing system.

Corresponding Author:

Chethan B. K.,
Department of Information Secience and Engineering,
Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India
Email: crsh2019@gmail.com

1. INTRODUCTION

Mobile Adhoc Network (MANET) is characterized by self-organizing node, decentralized architecture, and dynamic topology system [1, 2]. The networks in the MANET are unstructured and the nodes are mobile in nature hence it leads to security and performance issues [3]. Because of this, the Vulnerabilities may lead to fake messages, message eavesdropping, service denial or poor routing etc. Also, the MANETs are exposed to both the internal as well as external attacks [4]. In this regard, extensive studies on MANET are carried out since decades ago but still now no standard model is introduced in research domain [5, 6]. The reason behind issues in identifying the standard model is that viz. i) the energy, routing, traffic management, security problem, etc., are addressed separately but not combinely. There fore, research-based approach claiming to offer solution against one problem has actually ignored other problem because of which the solution cannot be considered in real-time applications. ii) Irrespective of security loopholes in MANET, the studies towards security problems are quite less in comparison to other problems from literature perspective. Majority of the security approaches in MANET are associated with routing schemes [7, 8] where complex encryption mechanism is the frequently adopted approach. When a mobile node starts moving at variable velocity, it not only drains its resources because of its attempt to establish connectivity during mobile state but also it drains significant resources due to incorporation of such complex encryption mechanism. iii) There is a closer relationship between the residual energy of mobile node with

consideration of security protocol running within the mobile nodes. Apart from transmittance and receiving energy allocation, a mobile node will also be required to expend energy for executing security protocol.

This is one big challenge in a long run especially for large scale network and resource constrained mobile nodes. Such considerations are found less involved in existing solution. iv) majority of the existing approach of network security in MANET is targeted towards mitigating a single form of adversary. It will mean that a solution to specific attack should also have to be proven if they are also capable of resisting other form of attack. There is no such evidence in any of the existing solution in this regards. A wireless network itself consists of multiple numbers of attacks and artifacts while transmitting data packets. There is single work that has offered solution towards indefinite or uncertain adversaries or if the strategies of attack is unknown while constructing the solution model. V) The application of MANET has a significant revolution as now MANET is considered as one of the integral part of upcoming technology Internet-of-Things (IoT). Therefore, when the mobile nodes are exposed to such technology than millions of adversaries are actually invited in the most vulnerable network. As IoT connects various heterogeneous domain (where MANET is just one domain of communication), hence of presence of any undetected adversary will also have a collateral damage of other form of communication domain connected in IoT. The security system in IoT is just a beginning and there are more concrete test-environment required to offer optimal security [9, 10].

Therefore, the proposed study introduces a framework that targets to conserve maximum resources along with offering more enhanced securing against maximum form of attack. The proposed study also presents an agent node with an agenda of reducing the computational effort of routing and security option in MANET. The paper presents a comprehensive discussion of a novel methodology where a lightweight security policy has been used in MANET. The organization of the paper is as follows: Section 1 discusses about the existing literatures where different techniques are discussed for detection schemes used in power transmission lines followed by discussion of research problems and proposed solution. Section 2 discusses about algorithm implementation followed by discussion of result analysis in Section 3. Finally, the conclusive remarks are provided in Section 4.

Existing approaches towards securing communication system in MANET is basically carried out using encryption-based approaches. The most recent work of Sowah et al. [11] have deployed a predictive approach for resisting man-in-middle attack in MANET. The authors have used neural network for developing intrusion detection system. Trust-based approach is another mechanism for securing communication system in MANET as seen in the work of Xia et al. [12]. Resisting black-hole attack has been discussed by Yasin and Zant [13] where bait on the basis of temporal factor has been used for detection and prevention. Kolandaisamy et al. [14] have offered a solution towards resisting distributed denial of service attack by analyzing the streams using statistical approach. The work of Kanagasundaram and Kathirvel [15] have claimed to offer security ofer famous OLSR protocol considering both energy and security aspect. Trust-based approach towards three distinct layers (physical, network, and MAC) has been carried out by Ghugar et al. [16] focusing on resisting jamming / cross-layer attack in adhoc network. Ahmed et al. [17] have also used trust-based scheme considering vehicular network.

Adotion of evolutionary technique is also found to contribute towards securing communication in MANET system. The works carried out by Elwahsh et al. [18] have jointly used evolutionary approach as well as machine learning approach for classifying the adversaries in MANET. Jadoon et al [19] have discussed the usage of lightweight encryption scheme towards securing MANET. A unique framework is modeled by Smith et al. [20] for facilitating existing approaches for amending their security mechanism. Luong et al. [21] have used machine learning approach for resisting flooding attack in MANET. Key management approach is another frequently used mechanism towards security in MANET. Ramkumar and Singh [22] have used Chebyshev polynomials for boosting the key management strategies in MANET. Extracting entropy information of the communication state in MANET was also claimed to enhance the encryption method in MANET as seen in work of Reshmi and Murugan [23]. Khan et al. [24] have used permutation of encoding vectors that was claimed to offer better complexity control while performing encryption in MANET.

Novotny et al. [25] have used Bayesian reasoning approach for controlling the fault tolerance factor in MANET that indirecty supports better security system. Study towards involving channel capacity and delay while forming the enhanced network secrecy was seen in work of Cao et al [26]. Adoption of middleware system is also claimed to offer better security system in adhoc network as the authors Silva and Albini [27] claimed to enhance the key management operation in MANET. Dynamic key management approach towards resisting key-based attack was discussed by Chen et al. [28]. Ghosh and Datta [29] have presented a model where the address information of the mobile nodes is secured against all the existing security challenges in MANET. Zhang et al. [30] have used an approach to resist jamming attack using

distribution of spread codes in MANET. The research problems associated with existing approaches are briefed in next section.

The significant research problems are as follows:

- Existing approaches are directly targeting to prevent the adversary with predefined information about it, which is quite unpractical.
- Adoption of cryptographic approach offers security but it also consumes time and resources that have not been discussed much in existing security approaches.
- There are few studies that have introduced usage of external agent (e.g. middleware) for contributing security enhancement in MANET which has a large scope in future.
- Majority of the approaches uses key management technique where the key security is not discussed in presence of dynamic attacks in MANET.

From the above points it is found that there is a need of "*Developinga framework that offers extensive saving of resources while promoting better communication performance and security feautures in presence of dynamic attack is quite challenging".*

The proposed system is aimed to ensure the safest communication among the mobile nodes in MANET by offering preventive measures towards the accessibility of the intruder. Hence, a lightweight encryption approach is introduced in which equally emphasize on resource saving and faster communication along with security upgradation. Figure 1 highlights proposed implementation scheme.

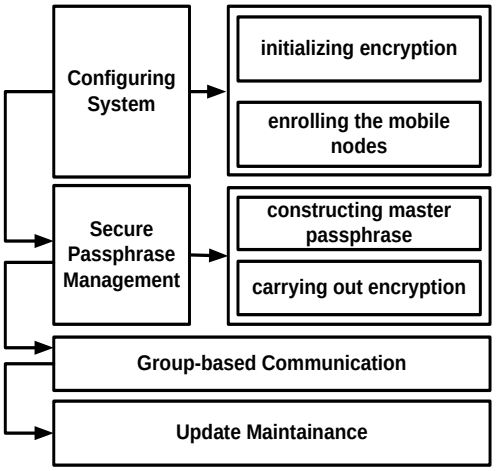

Figure 1. Proposed implementation scheme

The proposed implementation is carried out considering analytical methodology where the prime focus in towards introducing novel system parameters for boosting up lightweight encryption. The first block of conguration of system is responsible for introducing such parameters to ensure forward and backward security while performing encryption which is the novelty of the system. The secure passphrase management block is meant for utilization of passphrase to achieve higher degree of confidentiality and non-anonymity during data transmission. The third block is about group-based communication system which is responsible for offering structured communication system using geographically located agent nodes with mobile nodes in MANET. Finally, the fourth block of update maintainance is responsible for offering security of all the security tokens that has been used so that no attacker could gain benefit out of it. The novelty of this model is that it offers multiple levels of security which makes the attacker quite challenging to break in the network. The next section discusses about system implementation.

2. SYSTEM IMPLEMENTATION

The complete system implementation is designed on the basis of the establishing secured connection between agents and mobile nodes in MANET environment. The design principle emphasizes on implementing a lightweight encryption policy where a structured form of grouping of the IoT nodes are carried out for streamline communication system. This section outlines are essential information associated with implementation.

2.1. Core parameters

There are 3 core parameters involved in the proposed system as follows- i) *mobile nodes*- they are conventional mobile nodes of MANET that are deployed randomly in the simulation area and they performs group wise communication system, ii) *agent nodes*-they a specific form of nodes that area geographically positioned within the simulation area. An interesting fact of this agent node is that a unique form of mobility concept is incorporated in proposed system. It is believed that making the agent node mobile will also drain the resource of agent nodes in long run and such energy can be retained to large extent if agent nodes are made stationary. However, making the agent node to be stationary will also have its limitation with respect to the coverage. Therefore, the proposed system offers the capability to distribute many numbers of agent nodes, but the agents nodes are controlled to be working on active mode by the user remotely.

This process saves unwanted energy drainage of the agent nodes in practical environment of MANET, iii) *security token matrix*: Basically, this master matrix retains information about four different types of security tokens e.g. *initial passphrase* (α_1), *shared passphrase* (α_2), *adjacent passphrase* (α_3), and *group passphrase* (α_4). The *initial passphrase* (α_1) is basically a security token generated by trusted authority (i.e. IoT gateway node) to all the mobile nodes. The *shared passphrase* (α_2) is a shared unique security token between all the mobile nodes and agents with IoT gateway. The *adjacent passphrase* (α_3) is shared unique security token between two mobile nodes either in same or in different domain system. The *group passphrase* (α_4) is security token used for encrypting forwarded information of specific group from mobile nodes to agent node. The pictorial representations of the parameter are shown below in Figure 2.

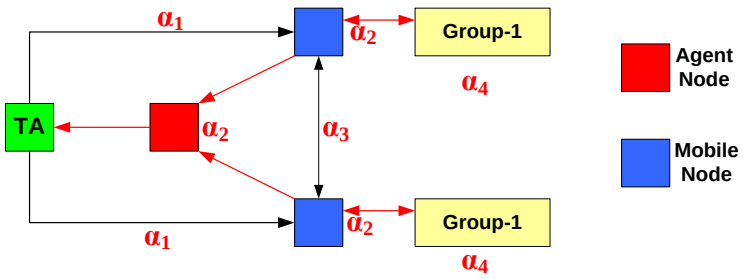

Figure 2. Usage of proposed security token principle

2.2. Implementation strategy

As the proposed system targets to achieve lightweight security policy, the implementation strategy involves usage of such passphrase irrespective of conventional secret key. The logic is conventional usage of secret key is basically derived from passphrase. Moreover, usage of passhrase offers more control over security access and itsinternal operation as compared to secret key. Apart from this fact, the passphrase have flexible sizes (which could be controlled by user also) while secret key sizes are always constant and this aspect could tremendously offer significant reduction in computational complexity irrespective of using encryption-based approach in proposed system. All the mobile nodes as well as agents are required to be enrolled with respect to gateway node which leads to the process of generation of various forms of security tokens. The complete communication is – A group-based communication system is initiated where all the mobile nodes split up to form different domains (or group). Each domain is allocated with a single agent node which captures data from its respective domain nodes. It is assumed that all the agents are updated by exchanging periodic sync messages internally among themselves. Finally the agent forwards the aggregated data to the IoT gateway that is further followed by spontaneous updating of the security token. Apart from this strategy, the proposed system also implements a mechanism that allows the agent to facilitate identification of old node leaving the domain or new node joining the domain.

2.3. Execution process

By adopting the novel parameters, the proposed system accomplishes its execution towards securing the communication system in MANET. Following are the process involves in proposed execution:

- ***Configuring System*:** This process includes two sub-process deployment viz. *initializing encryption* and *enrolling the mobile nodes*. The encryption process is initialized by applying hash operation over finite field and passphrase generated by trusted authority. The computation of the final passphrase is carried out by scalar multiplication of master passphrase with attribute of finite field. The gateway forwards this final outcome of hashing privately to all mobile nodes. The next operation is that of enrolling mobile nodes

where a unique tag is allocated for both mobile node and agent node. The mobile node computes passphase using its secret arbitrary number. Using similar parameters, the IoT gateway generates only half of the passphrase using a random value which is validated by mobile nodes. The validation is only said to hold successful if scalar multiplication of distance of specific mobile node and global passphrase is found equivalent to summation of random value of mobile node and hashed value of passphrase of that node.

- ***Secure Passphrase Management*:** This process consist of two sequential operations i.e. constructing *master passphrase* and *carrying out* encryption. In this process, the transmitting node forwards a request message which upon getting a response from the neighboring mobile nodes forwards the data in encrypted form. The transmitting node constructs a secret passphase by applying hashing over global passphrases of both transmitting and receiving mobile node. Upon receiving this message, the receiving mobile node starts decryption process by extracting the hash value of the embedded message. A specific condition is formulated where the receiving node checks by summing up random value of transitting node and hash value of all the local and global passphrases. In case of valid outcome, the receiver nodes finalize the decryption process or else discard the message. This step ensures proper validation of the messages in case of receiving a spurious message from any mobile node. Finally the encryption process can be carried out using any encryption method using the same passphrase that it has been used in prior step.
- ***Group-based Communication*:** In order to maintain a streamline communication system, the proposed system performs group-based data transmission. The initiation of the group formation is carried out by agent node. After the agent nodes obtains the internal message from the mobile node, it initiates its processing of the validating that node. The group-based communication is carried out by discovering the mobile nodes followed by validating them. The group nodes then generate the secret passphrase and transmit it to all the mobile nodes in its respective domain. The receiver mobile node deciphers the received message. Upon deciphering, if the receiver node finds the other node malicious than it updates the agent node which further quarantine the malicious node from participating in data forwarding process. Once the explorations of all the respective mobile nodes are accomplished than the agent node computes another passphrase and forward it to the gateway node. As the gateway node maintains list of all the legitimate mobile nodes, so it can offer it conformity to the agent node. The gateway node also updates the list of suspicious / malicious intruder to other mobile agents in order to protect from any further case of concurrent adversaries in MANET. After this process, the communication is continued among the mobile nodes via agent nodes in deployment area.
- ***Update Maintainance:*** Updating is an essential operation in MANET as existing routing scheme in it suffers from faster upgrade transmission. Therefore, proposed system offer emphasis to the updating process for the encrypted passphrases in order to resist them from being accessed / compromised. The proposed system doesn't require adjacent passphrase for many number of updates as it is not directly in all communication process. The usage of master adjacent passphrase is only required if one of the mobile node is compromised or about to get compromised. In case of attack event report, this passphrase is instantly updated to all the domains. The next task is to update the group passphrase. According to proposed system, the agent node has the authorization to update the group passphrase and none of the mobile node is actually authorized to amend / change the group passphrase. If they do so than it will be considered as an adversary. In such case, a new group passphrase is calculated by the associated agent node along with generation of new flag for updating the prior passphrase. The entire mobile node after receiving the update message performs deciphering to check the authentication of it followed by further upgrading their shared passphrases. This operation is also carried out for the old mobile node leaving the prior domain and new mobile node joining a new domain. This is carried out by consulting the master matrix which retains all the final passphrase update information resulting in faster updating process for all the agent nodes as well as mobile nodes in MANET environment. This makes the proposed system offer extensive security.

From the complete logic written above, it can be understood that proposed system performs a sequential implementation of this execution process. The algorithm for establishing secured communication in proposed system and its execution steps are as follows:

Algorithm for Establishing Communication

Input: p (MANET nodes), q (agent)
Output: com (communication vector)
Start
1. *init* → deployment rand(p), uniform(q)
2. *generate* → θ=[a|b]

3. **For** i=1:p
4. **For** j=1:q
5. K→*f*(x) //311
6. **For** dist<R
7. form group=[struct(dist)]
8. **End**
9. select→ best *q*
10. com=p(group)→*q*
11. **End**
12. **End**

End

The algorithm takes the input of *p* (MANET nodes) and q (mobile agent) which after processing yields and outcome of *com* (communication vector). The first step of the proposed algorithm is to perform uniform deployment of agent node and random deployment of mobile node (Line-1). The study then formulates various security attributes viz. the first attribute *a* represents parameters of system which are going to be used in encryption process while the second attribute *b* represents hashed value of the prior attributes. The concatenation of both the attributes generates a unique value θ (Line-2). The proposed algorithm is carried out considering all the mobile nodes as well as agent nodes. Considering all the system attributes, the proposed system applies a function *f*(x) that generates the master secret passphrase *K* (Line-5). The computation of this *K* is carried out by scalar multiplication of hashing value and system attributes along with consideration of destination node. However, this computation of *K* is only permissible if the request generated by transmitting node is found to be valid. One of the interesting things to observe is that there are multiple layers of encryption carried out by hashing over multiple parameters in different way. Hence, even if it is assumed that there is a man-in-middle attack or any other form of internal attack, only the small part of the ciphered information will be compromised. In order to decrypt that small part of ciphered content, the adversary will require obtaining access to master passphrase as well as all the other encrypted attributes. This operation will require a malicious node to expend maximum resource and hence it is less likely that malicious node will be every successful to decrypt the ciphered data.

The algorithm then constitutes a group on the basis of the distance dist where all the nodes less than defined communication range *R* of the agent node constitute a group (Line-6). In order to deal with the computational complexity problem, the algorithm also contructs a structured group (Line-7) which is carried out on the basis of the distance. This will mean that all the agents will have sync among themselves and starts processing the request for new node joining the network. After the secure passphrase is generated by the agent node, it is forwarded to mobile nodes which execute the process in order to perform communication. However, in this process, not all the agent nodes will be required. Therefore, the proposed system chooses the best agent nodes (Line-9) on the basis of the distance. It will mean that only the agent nodes with higher density of communicating nodes will be used and others will have to turn off its radio system. There fore, group is formulated only for the active agent nodes. The algorithm finally establishes a communication vector *com* between the mobile nodes via agent nodes using either single / multihop network system in MANET. Therefore, it can be said that a good amount of resources are conserved for the agent nodes while performing the process of information propagation in MANET. A closer look in this algorithm will also show that proposed system doesn't use anyform of complex cryptographic system other than using hashing operaion. Hence, the size of the ciphered content will be significantly reduced which will offer better bandwidth utilization as well as lesser resource dependency. Moreover, the algorithm is constructed in such a way that it is nearly impossible to decrypt any chunk of encrypted file in the entire process. Therefore, the algorithm can be claimed to offer an extensive security irrespective of the kind of attack in existing system. The next section outlines the results obtained.

3. RESULT ANALYSIS

The analysis of the proposed system is carried out in MATLAB considering 100-500 number of mobile node and 10-100 number of agent nodes. This initialization of mobile nodes and agent nodes comes in ratio of 1:10 respectively. Apart from this, the outcome of the study is compared with existing secure routing scheme in MANET e.g. SAODV [31] and SLSP [32] considering delay, residual energy, key generation time, and key validation time. Figure 3 and Figure 4 showsthat proposed system offers reduced delay as well as higher residual energy in contrast to existing system. The reason of reduced delay is due to incorporation of the agent nodes for facilitating faster authentication services to the mobile nodes. Reduced energy consumption results because of two factors viz.i) agent nodes which works on demand based on the density

of traffic and ii) usage of hashing operation in multiple level which offers good balance between energy consumption and higher security features. Figure 5 and Figure 6 highlights that proposed system offers reduced time for generating the security token in contrast to existing security system. The prime reason behind reduced time are many viz i) usage of hashing make the encryption lower in size thereby making the transmission faster and ii) usage of master security token by the agent nodes reduces the time and effort of the validation by normal mobile nodes. The validation time is calculated as the time after receiving the security token till the flag message generated for declaring successful/failed validation. The validation time of the proposed system is also reduced for similar reason. Unfortunately, existing system doesn't have any inclusion of agent which eventualy proves that incusion of agent significant prove the communication performance of mobile nodes with security.

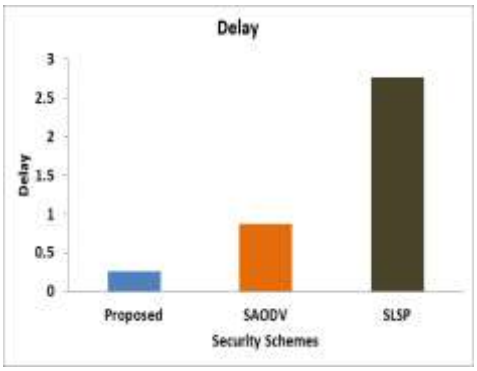

Figure 3. Comparative analysis of delay

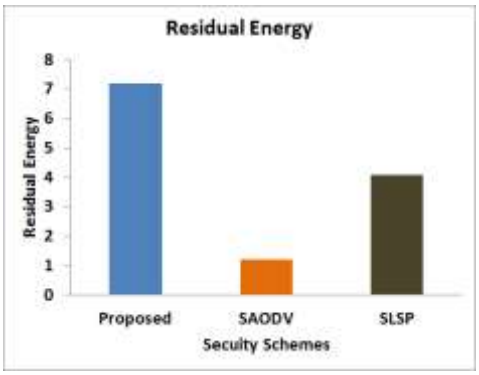

Figure 4. Comparative analysis of residual energy

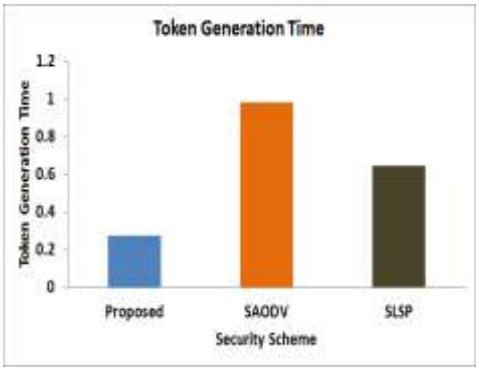

Figure 5. Comparative analysis of key generation time

Figure 6. Comparative analysis of validation time

4. CONCLUSION

The various approaches used in existing system towards counter measuring adversaries are either cryptographic based or non-cryptographic based. However, cryptographic based solutions are dominantly used owing to the capability of algorithm to resist specific forms of attack. However, existing cryptographic algorithm are designed without considering the consequences of using complex encryption or resource usage of the mobile nodes. This problem in addressed in proposed system where the contributions are as follows: (a) An agent node has been used as a bridge of communication across multiple domain and thereby it supports large scale deployment; (b) Enough attention is also given for agent nodes which works on demand and not all the agent nodes are required to be functional; (c) The security algorithm is mainly executed by the agent nodes and partially by the mobile nodes, hence, even if any one mobile node is compromised or there is an instance of packet drop the entire network is secured; (d) Another significant novelty is that proposed system doesn't use key but uses passphrase which is not only smaller in dimension but also are programmable only by the legitimate nodes. Hence, the proposed system offers significant supportability towards dynamic attack. The future line of research can consider the proposed model with other security providing techniques along with machine learning approaches and achieve even more performance enhancement.

REFERENCES

[1] Dr. Humayun Bakht, "Applications of Mobile Ad-hoc Networks", CreateSpace Independent Publishing Platform, 2018.

[2] Jonathan Loo, Jaime Lloret Mauri, Jesús Hamilton Ortiz, "Mobile Ad Hoc Networks: Current Status and Future Trends", CRC Press, 2016.

[3] H. Moudni, M. Er-rouidi, H. Mouncif and B. E. Hadadi, "Secure routing protocols for mobile ad hoc networks," *2016 International Conference on Information Technology for Organizations Development (IT4OD)*, Fez, pp. 1-7. 2016.

[4] R. Meddeb, B. Triki, F. Jemili and O. Korbaa, "A survey of attacks in mobile ad hoc networks," *2017 International Conference on Engineering & MIS (ICEMIS)*, pp. 1-7. Monastir, 2017.

[5] S. Habib, S. Saleem and K. M. Saqib, "Review on MANET routing protocols and challenges," *2013 IEEE Student Conference on Research and Developement*, pp. 529-533. Putrajaya, 2013.

[6] R. Pushparaj and M. Dinakaran, "Energy efficient routing issues and challenges in mobile Ad Hoc networks," *Second International Conference on Current Trends In Engineering and Technology - ICCTET 2014*, pp. 26-31. Coimbatore, 2014.

[7] R. Sheikh, Mahakal Singh Chande and D. K. Mishra, "Security issues in MANET: A review," *2010 Seventh International Conference on Wireless and Optical Communications Networks - (WOCN)*, pp. 1-4. Colombo, 2010.

[8] R. Mishra, S. Sharma and R. Agrawal, "Vulnerabilities and security for ad-hoc networks," *2010 International Conference on Networking and Information Technology*, pp. 192-196. Manila, 2010.

[9] A. Kamble and S. Bhutad, "Survey on Internet of Things (IoT) security issues & solutions," *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, pp. 307-312. Coimbatore, 2018.

[10] S. A. Kumar, T. Vealey and H. Srivastava, "Security in Internet of Things: Challenges, Solutions and Future Directions," *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 5772-5781. Koloa, HI, 2016.

[11] Sowah, Robert A., Kwadwo B. Ofori-Amanfo, Godfrey A. Mills, and Koudjo M. Koumadi. "Detection and Prevention of Man-in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in Artificial Neural Networks (ANN)." J*ournal of Computer Networks and Communications*, 2019.

[12] Xia, Hui, San-shun Zhang, Ben-xia Li, Li Li, and Xiang-guo Cheng. "Towards a Novel Trust-Based Multicast Routing for VANETs," *Security and Communication Networks*, 2018.

[13] Yasin, Adwan, and Mahmoud Abu Zant. "Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique." *Wireless Communications and Mobile Computing*, 2018.

[14] Kolandaisamy, Raenu, Rafidah Md Noor, Ismail Ahmedy, Iftikhar Ahmad, Muhammad Reza Z'aba, Muhammad Imran, and Mohammed Alnuem. "A multivariant stream analysis approach to detect and mitigate DDoS attacks in vehicular ad hoc networks." *Wireless Communications and Mobile Computing*, 2018.

[15] Kanagasundaram, Hamela, and A. Kathirvel. "EIMO-ESOLSR: energy efficient and security-based model for OLSR routing protocol in mobile ad-hoc network." *IET Communications*, Vol. 13, no. 5, pp. 553-559, 2018.

[16] Ghugar, Umashankar, Jayaram Pradhan, Sourav Kumar Bhoi, and Rashmi Ranjan Sahoo. "LB-IDS: Securing Wireless Sensor Network Using Protocol Layer Trust-Based Intrusion Detection System." *Journal of Computer Networks and Communications*, 2019.

[17] Ahmed, Sheeraz, Mujeeb Ur Rehman, Atif Ishtiaq, Sarmadullah Khan, Armughan Ali, and Shabana Begum. "VANSec: Attack-resistant VANET security algorithm in terms of trust computation error and normalized routing overhead." *Journal of Sensors*, 2018.

[18] Elwahsh, Haitham, Mona Gamal, A. A. Salama, and I. M. El-Henawy. "A Novel Approach for Classifying MANETs Attacks with a Neutrosophic Intelligent System based on Genetic Algorithm." *Security and Communication Networks*, 2018.

[19] Jadoon, Ahmer Khan, Licheng Wang, Tong Li, and Muhammad Azam Zia. "Lightweight Cryptographic Techniques for Automotive Cybersecurity." *Wireless Communications and Mobile Computing*, 2018.

[20] Hurley-Smith, Darren, Jodie Wetherall, and Andrew Adekunle. "SUPERMAN: Security using pre-existing routing for mobile ad hoc networks." *IEEE Transactions on Mobile Computin*, Vol 16, no. 10, pp. 2927-2940, 2017.

[21] Luong, Ngoc T., Tu T. Vo, and Doan Hoang. "FAPRP: A Machine Learning Approach to Flooding Attacks Prevention Routing Protocol in Mobile Ad Hoc Networks." *Wireless Communications and Mobile Computing*, 2019.

[22] Ramkumar, K. R., and Raman Singh. "Key management using Chebyshev polynomials for mobile ad hoc networks." China Communications, Vol 14, no. 11, pp. 237-246, 2017.

[23] Reshmi, T. R., and K. Murugan. "Light weight cryptographic address generation (LW-CGA) using system state entropy gathering for IPv6 based MANETs." *China Communications*, vol 14, no. 9, pp. 114-126, 2017.

[24] Khan, Ali, Qifu Tyler Sun, Zahid Mahmood, and Ata Ullah Ghafoor. "Energy efficient partial permutation encryption on network coded MANETs." *Journal of Electrical and Computer Engineering*, 2017.

[25] Novotny, Petr, Bong Jun Ko, and Alexander L. Wolf. "Locating Faults in MANET-Hosted Software Systems." *IEEE Transactions on Dependable and Secure Computing*, Vol.15, no. 3, pp. 452-465, 2016.

[26] Cao, Xuanyu, Jinbei Zhang, Luoyi Fu, Weijie Wu, and Xinbing Wang. "Optimal secrecy capacity-delay tradeoff in large-scale mobile ad hoc networks." *IEEE/ACM Transactions on Networking (TON)*, vol. 24, no. 2, pp. 1139-1152. 2016.

[27] da Silva, Eduardo, and Luiz Carlos Pessoa Albini. "SEMAN: A Novel Secure Middleware for Mobile Ad Hoc Networks." *Journal of Computer Networks and Communications*, 2016 .

[28] Chen, Chin-Ling, Chih-Cheng Chen, and De-Kui Li. "Mobile device based dynamic key management protocols for wireless sensor networks." *Journal of Sensors*, 2015.

[29] Ghosh, Uttam, and Raja Datta. "A secure addressing scheme for large-scale managed manets." *IEEE transactions on network and service management*, Vol. 12, no. 3, pp. 483-495, 2015.
[30] Zhang, Rui, Jingchao Sun, Yanchao Zhang, and Xiaoxia Huang. "Jamming-resilient secure neighbor discovery in mobile ad hoc networks." *IEEE Transactions on Wireless Communications*, Vol 14, no. 10, pp. 5588-5601, 2015.
[31] S. Lu, L. Li, K. Lam and L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," 2009 *International Conference on Computational Intelligence and Security*, Beijing, pp. 421-425. 2009.
[32] P. Papadimitratos and Z. J. Haas, "Secure link state routing for mobile ad hoc networks," 2003 *Symposium on Applications and the Internet Workshops*, Orlando, FL, USA, pp. 379-383. 2003.

BIOGRAPHIES OF AUTHORS

Chethan B.K is working as assistant professor department of information science and engineering in Sri Siddhartha Institute of Technology, Tumkur, India. He has around 12 years of teaching experice. His research domains are computer network, network security and software engineering. Currently, He is pursuing his phd from VTU, Belagavi, India

Dr. M. Siddappa is working as a dean academics, professor and head department of computer science and engineering in Sri Siddhartha Institute of Technology, Tumkur, India. He has total number of experience is 30 years. His research domains are computer network, Artificial Intelligence, Soft Computing and agent based systems.

Dr. H S Jayanna is working as a professor and head department of information science and engineering in Siddaganga Institute of Technology, Tumkur, India. He has total number of experience is 25 years. His research domains are computer networks, Pattern recognition, Image processing, Continuous speech recognition and Speaker Identification/Verification using speech.