JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Reduction Of Attacks In MANET-IoT Network By Identifying Critical Nodes - Using DCNI Methods And Rekeying Technique

[1]Dr. Janani V.S, [2]Aiswarya K, [3]Balaji S, [4]Dharani S

[1]Associate Professor, [2]Student, [3]Student, [4]Student
[1]Electronics and Communication engineering,
[1]Easwari engineering college, Chennai, Tamil Nadu, India

Abstract : In heterogeneous environments, the Internet of Things (IoT) with mobile ad hoc network (MANET), i.e., MANET-IoT network becomes attractive for users, and also it is economically successful. The introduction of MANET has made the system prone to attacks due to its lack of centralized management, weak connectivity, and resource limitations. To improve network scalability, the critical nodes of the MANET-IoT network should be identified and protected. Most of the methods for identifying critical nodes usually use the static network method or a single topology snapshot in dynamic networks without considering the relation between topology snapshots, which cannot improve the efficiency of MANET-IoT networks. A dynamic critical node identification (DCNI) method is proposed in this paper. Firstly, an extensive metric to measure the node importance in the topology snapshot is done. A sliding time window is used to eliminate the topology snapshots which correlate with the current snapshot and combine the importance values of the same node in different topology snapshots. Finally, the critical nodes are identified based on the result of fused importance. The port hopping mechanism can be used for the critical nodes to improve network defence. The results show that the proposed Dynamic Critical node method is very effective for identifying critical nodes than existing static and single topology methods in MANET-IoT networks, and the port hopping mechanism improves the network defence to denial of service (DoS) attacks. Rekeying technique will improve the stability of MANET-IoT and reduce the chances of error. Rekeying is an effective cryptographic key management system.

***IndexTerms* – MANET-IoT network architecture, topology snapshot, dynamic critical node identification, network defence, denial of service (DoS), port hopping mechanism, mobile computing, Rekeying.**

I. INTRODUCTION

The Internet of things (IoT) is a part of the since the field has evolved due to the convergence of multiple technologies. IoT enables each object to be connected to the Internet through sensors or chips without human interference. It includes different types of networks such as wireless sensor networks (WSNs), ZigBee, Wi-Fi, mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs). MANET in the IoT system is very attractive and easy to implement because it is a self-organizing and multi-hopping network, in which all nodes share a common channel and can move freely without the help of a fixed networking infrastructure. Moreover, MANET facilitates the development of new IoT communication platforms for a wide range of applications in different domains.

The MANET and IoT together create a new network called MANET-IoT network which gives greater mobility to end-users and reduces deployment costs. Due to the shortage of centralized management, weak connectivity, and resource limitations, MANET-IoT is more susceptible to attacks than other IoT networks. Importantly, the attacks to critical nodes may degrade the function of the network, such as disconnecting the network into multiple components, causing failure of cascading or even collapse the entire network, which ends up in issues for the MANET-IoT network. Therefore, it is important to identify and protect the critical nodes to improve the network defence.

Critical nodes identification is of two main categories: social network analysis and system analysis. Social network analysis is done by calculating statistics of certain attributes of the nodes; it evaluates and compares the importance of each node. The compared attributes can be divided into local metrics and global metrics, where the local metric is degree centrality and typical global metrics include various centralities like betweenness centrality, closeness centrality, eigenvector centrality, and few more. For system analysis, it reflects the destructive effects when a node is removed from the MANET-IoT network. System analysis avoids a few problems like the unreasonable choice of attributes and metrics in social network analysis. Currently, critical nodes identification has been studied in various research fields. However, all the researchers mainly specialize in static networks without considering the dynamic changes of topology.

II. LITERATURE SURVEY

For critical nodes in MANET, M. Sheng et al. proposed an algorithm based on a supported midpoint coverage circle (DMCC) to detect critical nodes. In DMCC, if a node i locate at the communication range of two nodes or all paths between two nodes pass-through node i, node i is identified as a critical node. Then, D. Zhang et al. proposed an alternate method to identify critical nodes in MANET, which adjusts value to the very close centrality and the betweenness centrality, instead of initial centrality. The critical nodes identified by adjusted betweenness centrality show the failure of an experiment by causing serious destruction to the network. The DMCC algorithm has improved the speed, reduced the detection load, and has improved the precision of calculating the centrality; these two experiments only identify the critical nodes of the current topology without considering the correlation between topology snapshots. Topology snapshot like the topology of MANET at a specific time point features a direct impact on the topology evolution at the subsequent time point. It only considers the current topology snapshot, the identification results will not be more precise enough to combine short lifetime links with long lifetime links, the importance of these short lifetime links is overemphasized. Due to the dynamic changes, the identified nodes might not be critical at the subsequent point. For MANET-IoT networks, there are various forms of attacks, such as denial of service (DoS) attack, eavesdropping, routing attack, black hole attack, wormhole attack, replay attack, and man-in-the-middle attack. Among all these, the denial of service (DoS) attack is one of the most common because of its low cost and easy implementation. To improve network defence, many strategies have been proposed, such as the removal of the crashed nodes, the allocation of limited defence resources, and the replication of robust data . However, these strategies require data to predict which nodes may fail in advance. Related researchers proposed various new security protocols, such as secure-aware ad hoc routing (SAR) protocol, secure efficient ad hoc distance vector routing (SEAD) protocol, authenticated routing for ad hoc networks (ARAN) protocol. These protocols are proved to slightly reduce the possibilities of attacks. Recently, Y. Jie et al. proposed a dynamic defence strategy for DoS attacks within the VANET supported port hopping, which detects and removes packets launched by attackers and doesn't make any change in the existing protocols. The port hopping mechanism is to vary the critical nodes' port numbers dynamically. For attackers, static ports can enable them to learn the characteristics of each port as time goes on. However, when the ports change the time, conducting an attack are going to be difficult, and therefore the critical nodes can filter off the attacks by checking the relevant port numbers.

In this paper, a method named dynamic critical node identification (DCNI) to identify the identification of critical nodes in MANET-IoT networks is proposed; the network defence of the whole network is enhanced to resist DoS. The following are the contributions of this paper:

1) A extensive metric to measure the nodes' importance in the static networks or the topology snapshot of dynamic networks is proposed.

2) A new method to identify critical nodes is proposed, by introducing a sliding time window, this method could effectively identify the critical nodes under the dynamic topology changes.

3) A port hopping mechanism to reinforce the network defence of MANET-IoT networks, which could reduce the success probability of DoS attacks.

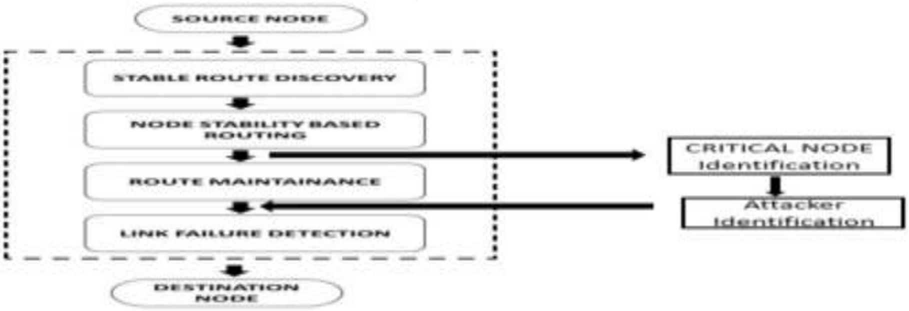
4) A effective rekeying key management system to secure the MANET-IoT

III. PROBLEM FORMULATION

It is considered that N homogeneous IoT networks are randomly connected in a two-dimensional area to form a MANET-IoT network, which is designed as a graph sequence denoted by G as in. The initial network at time point t_1 is designed as graph G_1 D $(V_1; E_1)$, where V_1 represents

The set of nodes in G_1, and E_1 represents the set of edges In G_1. The nodes in G_1 represent the IoT networks; meanwhile, the edges between nodes are the communication links between the IoT networks. If the received signal-to-noise ratio (SNR) is greater than the demodulation threshold, it is considered that there is a communication link between the networks. $e(u; v)$ is the Euclidean distance of the node u and v, r_m represents the communication distance. The network at the time point t_i is represented as G_i, and then a MANET-IoT network can be depicted as a sequence of network snapshots evolving all the time.

Considered a MANET-IoT network G, critical nodes identification is to realise the rank of the nodes with the help of the node importance values that are consistent with the relation between different topology snapshots and determine top k nodes as critical nodes for protection and safety.



IV. EVALUATION CRITERIA

To better identify critical nodes, the local connection attributes and the global location attributes are considered. We used different types of degree centrality and betweenness centrality to build extensive evaluation criteria.

4.1 Degree centrality

The degree centrality of the node reflects the number of edges connected associated with the node. In an undirected network, the number of neighbours with the node is equal to the node degree. For the given network, assume the number of nodes in the network as n and construct the adjacency matrix of the network.

The advantage is that the calculation is simple and also it reflects the relationship between the node and its neighbouring nodes. The disadvantage is that it cannot reflect the importance of the neighbouring nodes.

4.2 Betweenness centrality

To extend the life cycle of the network and save energy consumption, the routing protocol of the MANET-IoT network usually selects the shortest path between nodes for information transmission. The betweenness centrality of a node contains the fraction of all shortest paths in the network that goes through the node.

4.4 Extensive evaluation metric

The number of common neighbours reflects the strength of the connection between two different nodes[34]. The number of common neighbour nodes is large, then the connection is stronger. The degree centrality and betweenness centrality are comprehensively taken into account the advantages of degree centrality is local attribution and betweenness centrality is a global attribution.

The betweenness centrality can effectively reflect the role of the node in the whole network path. The disadvantage is that it does not reflect the tightness between the node and its neighbour nodes.

V. Node importance of fusion method

To effectively deal with the dynamic changes of topology, a sliding window method is proposed to identify the fusion of node importance in different topology snapshots.

5.1 Sliding window method

The sliding window is based on the number of items. There are W topology snapshots in the window at any time point, where w is the window width. According to the order of snapshots timestamps, they enter the sliding window which is represented as a topology sequence.

When the width is fixed, new data enters the window, and the stale data are deleted simultaneously. A topology snapshot at each time point is considered as the unit of data.

5.2 Fusion of importance

Node importance of snapshot: According to the topology snapshot the importance of a node is obtained at a time point is called the snapshot importance of a node.

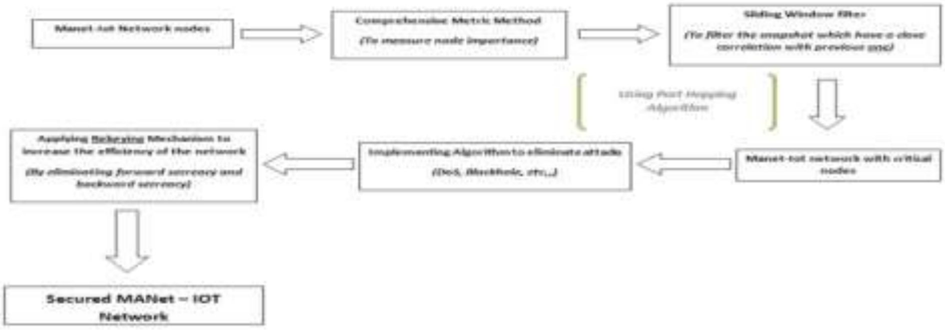
Dynamic Importance of the Node: All the snapshot importance of node VJ in time [0, ti] is fused, and the result is called the dynamic importance of the node at time point ti. The degree of attenuation is defined to measure the importance of snapshot importance at time points.

Attenuation Degree: At two adjacent time points ti−1 and ti, the importance of the node is attenuated by a proportional constant, which is called the attenuation degree and denoted as α, where $0 < \alpha < 1$.

5.3 Identification of window width value

The sliding window mechanism based on the data processing model uses a subset of data in calculation results, the accuracy of the result is affected by the width of the sliding window. To obtain the window width w, the distance attenuation coefficient ζ is assumed which is a sufficiently small positive number. $\alpha w \rightarrow 0$ becomes $\alpha w \rightarrow \zeta$, therefore, w = logα ζ . The window width w is only related to the user-set attenuation α and the distance attenuation coefficient ζ.

VI. Proposed DCNI method


Manet-IoT Network nodes
Comprehensive Metric Method
(To measure node importance)
Sliding Window filter
(To filter the snapshot which have a close correlation with previous one)
Using Port Hopping Algorithm
Manet-IoT network with critical nodes
Implementing Algorithm to eliminate attacks
(DoS, Blackhole, etc.,)
Applying Rekeying Mechanism to increase the efficiency of the network
(By eliminating forward secrecy and backward secrecy)
Secured MANet – IOT Network

The basic process of the proposed DCNI method are :

Step 1: Construction of the extensive evaluation metric to calculate the importance of nodes in the topology snapshot as snapshot importance;

Step 2: Construction of sliding window to filter the topology snapshots that have an important influence on the current identification of critical nodes and infuse the importance of the node from different topology snapshots as dynamic importance;

Step 3: Top k ranked nodes are selected as critical nodes concerning the ranking result of nodes' dynamic importance;

The complexity of DCNI mainly comes from the calculation f nodes' snapshot importance and the rank process of nodes' dynamic importance. Using the algorithm proposed to compute betweenness centrality, the complexity of calculation is approximately O(m′n), where m′ is the number of links in the network. And the complexity of calculating comprehensive centrality is approximately O(m′n2). In the process of ranking nodes' dynamic importance, the average time complexity is O(N log N) when using the Quicksort algorithm. In summary, the complexity of DCNI is approximately (mn2).

VII. PORT HOPPING MECHANISM

We have introduced the port hopping mechanism for critical nodes to enhance the defence of the MANET-IoT network. The main idea of the port hopping mechanism is to change the critical nodes' port numbers dynamically to reduce the attack. The advantage is it is easy to implement without modifying the protocols.

Different port numbers are selected in different time slots in the port hopping mechanism.

The arrival of the packet will take place near the boundary of the time slot, to reduce the problem of synchronization errors, two ports are used at the boundaries of time slots.

When an ordinary node communicates with the critical node, the critical node’s current port number Pi is determined using the shared cryptographic secret key k and the time slot Si. The packets will be discarded when the critical node receives a packet that carries the wrong port numbers. The critical node does not analyze whether the packet contains malicious content, the consumption of computing resources is reduced and also detection time is reduced significantly.

The asymmetric key mechanism is adopted to share the cryptographic key between the node and the critical node. Each node shares a master key K with the critical node. Firstly a request pack is sent to the critical node when an ordinary node communicates with the critical node.

VIII. NETWORK SIMULATION

First, we conduct a few experiments in some public static network data and static MANET-IoT to identify the feasibility of DCNI in identifying the critical nodes. In a static network, the DCNI method is equivalent to using the extensive metric proposed in the paper to evaluate the node's centrality. We add a mobility model to the nodes and, conduct experiments to verify the ability of DCNI to speed up with the dynamic topologies.

Finally, a few experiments are conducted to compare the defence Ability change of the MANET-IoT network and to check whether the port hopping mechanism is adopted by the critical nodes. The experiments could further analyse the importance of the identified critical nodes and play a vital role in enhancing MANET-IoT network defence

Checking authentication, if any one unauthorized it fixed as malicious and key Updation

IX. PERFORMANCE ANALYSIS

9.1 Result analysis of DCNI in static mode

The simulation of the MANET-IoT network was done by Network Simulator Version 2 (NS2), which is a simulator in wireless communication. All the nodes are deployed in the region, and the topology snapshot corresponding to the location of the nodes is considered. Various methods are applied to identify the rank of the nodes in static networks. The nodes are removed according to the rank, the changes of the network.

The nodes are removed according to the rank of DCNI, it declines faster than other methods. Experimentally we can prove that the DCNI method can be implemented in static networks and the rank is better than other methods.

9.2 Result analysis of DCNI in dynamic mode

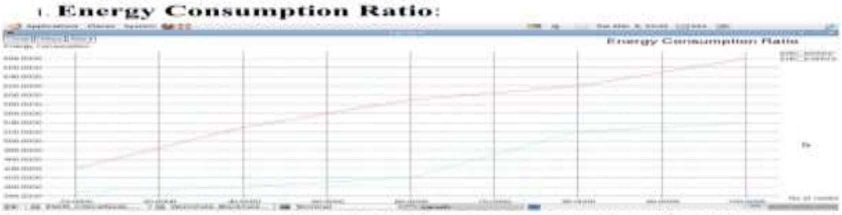
For generating a dynamic network, we have generated removal and addition of nodes in a random way for the terrorist network. This method identifies the dynamic changes in network topology, the location of the nodes is not considered. When a node moves, it will construct a link between the nodes near it mostly, and it will not connect to other nodes randomly. For better consideration of the correlation between topology snapshots, the reference point group mobility (RPGM) model [] is proposed to realize the dynamic changes of topology in the MANET-IoT network. The moving speed of the nodes ranges from [1, 10] m/s.

9.3 Determination of important parameters

In the process of infusing the importance of the node in different topology snapshots, the final fusion effect is directly affected by the value of w. If the value of w is too small, then the topology snapshots will have a great impact on the time point which cannot be filtered out. If the value of w is too large, then the stale topology snapshots reduce the accuracy of the final results.

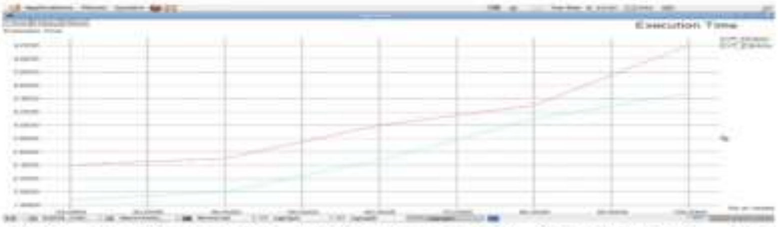
When the value of w is fixed, the node importance is mainly affected by α. The value of α is taken when the size of the largest cluster RI is minimum. When α is fixed, the difference of ζ determines the sliding window width, and the method for the determination of ζ is same as α. The value of RI will decreases because the stale topology snapshots directly affect the accuracy of the current time point.

1. **Energy Consumption Ratio:**



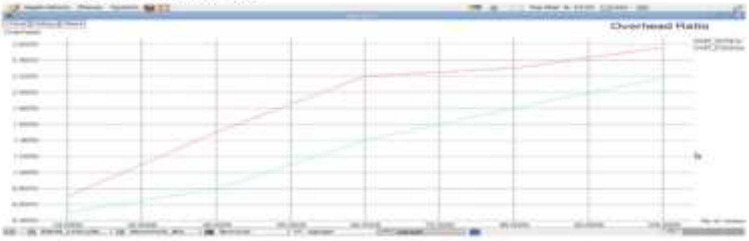
Here we comparing Energy Consumption for Existing, and proposed. In our modification life time ratio increased comparing to existing and proposed methods.

2. **Execution Time:**



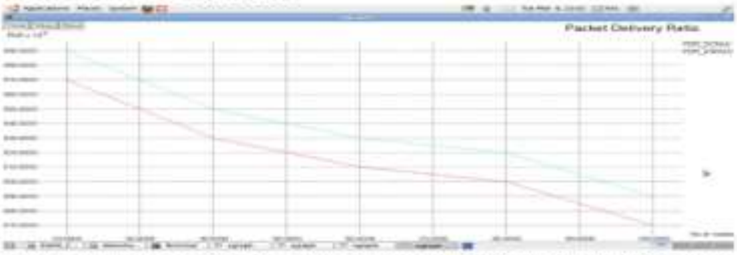
Here we comparing Execution Time for Existing, and proposed. In our modification life time ratio reduced comparing to existing and proposed methods.

3. **Overhead Ratio:**



Here we comparing Overhead Ratio for Existing, and proposed. In our modification life time ratio reduced comparing to existing and proposed methods.

4. **Packet Delivery Ratio:**



Here we comparing Packet Delivery Ratio for Existing, and proposed. In our modification life time ratio increased comparing to existing and proposed methods.

9.4 Analysis of the experimental results

The top-20 nodes after the rank allocation are selected as critical nodes. The timeliness and stability of dynamic critical nodes are considered, the overlap ratio is the measure of identification results of dynamic critical nodes which are denoted as RV.

More than a hundred simulations were done for each experiment at different time points to identify the critical nodes. The results were compared with the static critical nodes results in the topology snapshot of various time points, and the average overlap ratio was calculated.

The lifecycle of critical nodes is very short. The dynamic critical nodes maintain a very high overlap ratio because of the DCNI method. In the comparison with topology snapshots, the overlap ratio reaches more than 70%, while the critical nodes selected by the other methods show a shorter life span, and only maintain a high overlap ratio with the nearest topology snapshot.

The critical nodes are removed in the topology snapshot of the next 10 time points for the critical nodes selected at specific time points by different methods and the average of RI is calculated. The critical nodes selected by DCNI are more efficient than other static methods.

9.5 Result analysis of port hopping mechanism

When the defence strategy based on the port hopping mechanism is adopted or not, the defence ability of the MANET-IoT network is different. To measure the port hopping mechanism on the network defence, we test the influence of the DoS attack in two different ways; attack a single critical node, the other is to attack multiple critical nodes.

In a single attack, the percentage of the packets sent from various nodes that have been received is measured, and the test is performed with and without the port hopping mechanism.

In a single attack victim, the attacker selects one attack target, and 100 attacks were conducted. The port hopping mechanism shows significant performance improvement. Without port hopping, the performance is decreased to below 30%.

And when the attack traffic reaches 450 kbps, the attack victim cannot receive during the scenario running time, which is treated as a failure node. In the port hopping mechanism, the node can receive nearly 60% of good traffic.

In multiple victims, the top-ranked critical nodes are attacked in the network, if the target has failed, then the next node becomes the attack victim, the attack traffic is 410 kbps. When a node fails, we consider that the links connected are disconnected.

The critical node does not adopt the port hopping mechanism, when 10 nodes are attacked, the network stability decreases below 50%. In the network, because of the limitation of resources, when one node fails, the processing capacity of the neighbouring nodes will also fail, this phenomenon is called cascading failure [33]. From the results, we can see that the congestion in the MANET-IoT network caused by DoS attacks can be significantly reduced with the help of a port hopping mechanism.

X. Conclusion

In this paper, we have studied the problem of identifying the critical nodes in MANET-IoT networks, and the dynamic critical node identification (DCNI) method is proposed. The rekeying technique is also studied and implemented to secure the MANET-IoT and also various attacks like a black hole and DoS is reduced. The efficiency of the sliding time window to realize the fusion of node's importance in different topology snapshots is done. The DCNI method has effectively coped with the dynamic changes of topology in the network. Based on the results of the DCNI method, the improved version of the port hopping mechanism is introduced to critical nodes. The experiment has improved the effectiveness of the DCNI method on MANET-IoT networks in terms of solution quality and time complexity, the port hopping mechanism used by critical nodes has enhanced the stability of the MANET-IoT network and reduced DoS attacks significantly.

XI. Acknowledgment

The authors gratefully thank the reviewers for their valuable comments and suggestions.

XII. References

[1] Y. Zhang and O. Yagan, ‘‘Robustness of interdependent cyber-physical systems against cascading failures,’’ IEEE Trans. Autom. Control, vol. 65, no. 2, pp. 711–726, Feb. 2020

[2] S. K. Goudas, P. I. Dallas, S. Chatziefthymiou, and S. Kyriazakos, ‘‘A survey of IoT key enabling and future technologies: 5G, Mobile IoT, semantic Web and applications,’’ Wireless Pers. Commun., vol. 3, pp. 1–31, 2017.

[3] [2] X. Cheng, F. Lyu, W. Quan, C. Zhou, H. He, W. Shi, and X. Shen, ‘‘Space/aerial-assisted computing offloading for IoT applications: A learning-based approach,’’ IEEE J. Sel. Areas Commun., vol. 37, no. 5, pp. 1117–1129, May 2019.

[4] R. Chen, Z. Tian, H. Zhou, and W.-X. Long, ‘‘OAM-based concentric spatial division multiplexing for cellular IoT terminals,’’ IEEE Access, vol. 8, pp. 59659–59669, 2020.

[5] W. S. Alnumay, U. Ghosh, and P. Chatterjee, ‘‘A trust-based predictive model for mobile ad hoc network in Internet of Things,’’ Sensors, vol. 19, no. 6, pp. 1–14, 2019.

[6] W. Zhuang, Q. Ye, F. Lyu, N. Cheng, and J. Ren, ‘‘SDN/NFV-empowered future IoV with enhanced communication, computing, and caching,’’ Proc. IEEE, vol. 108, no. 2, pp. 274–291, Feb. 2020.

[7] T. Alam and B. Rababah, ‘‘Convergence of MANET in communication among smart devices in IoT,’’ Int. J. Wireless Microw. Technol., vol. 9, no. 2, pp. 1–10, Mar. 2019.

[8] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, ‘‘Convergence of MANET and WSN in IoT urban scenarios,’’ IEEE Sensors J., vol. 13, no. 10, pp. 3558–3567, Oct. 2013.

[9] B. Rasa, N. Lina, and A. Tomas, Ad Hoc Networks. Rijeka, Croatia: InTech, 2017, ch. 5, pp. 89–114.

[10] N. Zanoon, N. Albdour, H. S. A. Hamatta, and R. M. Al-Tarawneh, ‘‘Security challenges as a factor affecting the security of MANET: Attacks and security solutions,’’ Int. J. Netw. Secur. Appl., vol. 7, no. 3, pp. 1–13, 2015.

[11] A. Singh, D. M. Kumar, R. Rishi, and D. K. Madan, ‘‘A relative study of MANET and VANET: Its applications, broadcasting approaches and challenging issues,’’ Adv. Netw. Commun., vol. 132, pp. 627–632, 2011.

[12] M. Lalou, M. A. Tahraoui, and H. Kheddouci, ‘‘The critical node detection problem in networks: A survey,’’ Comput. Sci. Rev., vol. 28, pp. 92–117, May 2018.

[13] B. Wang, Z. Zhang, X. Qi, and L. Liu, ‘‘Identify critical nodes in network cascading failure based on data analysis,’’ J. Netw. Syst. Manage., vol. 28, no. 1, pp. 21–34, Jan. 2020.

[14] W. Jia-Sheng, W. Xiao-Ping, Y. Bo, and G. Jiang-Wei, ‘‘Improved method of node importance evaluation based on node contraction in complex networks,’’ Procedia Eng., vol. 15, pp. 1600–1604, Jan. 2011.

[15] M. Ventresca and D. Aleman, ‘‘Efficiently identifying critical nodes in large complex networks,’’ Comput. Soc. Netw., vol. 2, no. 1, p. 6, Dec. 2015.

[16] P. Bonacich, ‘‘Factoring and weighting approaches to status scores and clique identification,’’ J. Math. Sociol., vol. 2, no. 1, pp. 113–120, Jan. 1972.

[17] L. C. Freeman, ‘‘A set of measures of centrality based on betweenness,’’ Sociometry, vol. 40, no. 1, pp. 35–41, 1977.

[18] L. C. Freeman, ‘‘Centrality in social networks conceptual clarification,’’ Social Netw., vol. 1, no. 3, pp. 215–239, Jan. 1978.

[19] M. Girvan and M. E. J. Newman, ‘‘Community structure in social and biological networks,’’ Proc. Nat. Acad. Sci. USA, vol. 99, no. 12, pp. 7821–7826, Jun. 2002.

[20] L. Katz, ‘‘A new status index derived from sociometric analysis,’’ Psychometrika, vol. 18, no. 1, pp. 39–43, Mar. 1953.