Int. J. Communications, Network and System Sciences, **2013, 6, 176-185**
http://dx.doi.org/10.4236/ijcns.2013.64021 Published Online April 2013 (http://www.scirp.org/journal/ijcns)

Scientific Research

A Survey of MANET Survivability Routing Techniques

Malik N. Ahmed[1], Abdul Hanan Abdullah[1], Ayman El-Sayed[2]
[1]Faculty of Computer Science & Information System, University Technology Malaysia (UTM), Johor, Malaysia
[2]Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menouf, Egypt
Email: naaemalik2@live.utm.my, hanan@utm.my, ayman.elsayed@el-eng.menofia.edu.eg

Received February 17, 2013; revised March 18, 2013; accepted April 8, 2013

ABSTRACT

Mobile ad hoc networks have a wide range of application usage today, due to its great services, easy installation and configuration, and its other distinctive characteristics. In contrast, the attackers also have developed their own way to disrupt MANET normal operations. Many techniques, approaches and protocols have proposed to support Mobile Ad hoc Network (MANET) survivability in adversarial environment. Survivable of routing operations is the key aspects of the challenge in MANETs because most of destructive attacks classified as active attacks and all are intent to attack MANET routing operation to prevent it from providing it services in a right time. In this paper, we will discuss the most effective and practical initiatives have designed to keep MANET survive in an adversarial environment and how it supporting MANET availability.

Keywords: MANET; Survivability; Routing Techniques

1. Introduction

In some situations when there is an urgent need for network communication between collection of hosts but centralized administrator and fixed infrastructure are unavailable or difficult to deploy that means it is time for mobile ad hoc network. MANET has many characteristic which make it suitable for some important applications and it can provide services well in such cases.

Mobile ad hoc network have become an important part of our life due to its vital services which provided to the population and society. It used at home, work, emergency situation, and natural disaster. On the other hand, the threats of MANET have flourished too. There are several types of attacks and intrusions targeting wireless networks as general especially mobile ad hoc network because of the nature of its work [1-3]. These attacks directly affect the performance and the survivability of MANETs. There are many efforts have done to surviving MANETs and keep them to provide services even in the presence of intrusion and DoS attacks.

Routing is essential service for end-to-end communication in MANET, attacks on routing protocol disrupt the reliability and performance of MANET. It can be divided into two categories, first is routing disruption attack which the attacker trying to change the course of packets. Second resource consumption attack, the attacker inserts packet into the network to consume resources [4].

Attacks on MANET are classified as Active and Passive attacks [5], passive attacks are not dangerous if the delivering data is important than its security, because it does not affects the normal operation of MANET, while active attacks affecting the normal operation of MANET In several ways. This survey focusing on initiatives which make MANET survives against active attacks including Denial of Service (DoS).

The contribution of this survey are: 1) investigation of the most valuable techniques and approaches which support MANET routing survivability; 2) identification the requirement of routing survivability; 3) investigation of main DoS which violate availability; 4) the classification of routing survivability in initiatives in three groups: authentication, path selection, and attack detection. The rest of this survey is organized as follows: Section 2, MANET survivability requirement; Section 3, DoS attacks and its classification in Section 4. In Section 5, discussed the routing survivability initiatives. Section 6, General discussion and open points, and conclusion in Section 7.

2. Requirements for MANET Routing Survivability

Survivable network must adapt nodes transmit powers to ensures the continuation of mobility operations and it

must be able to change addressing and service recovery dynamically. When system is under attack nodes must use power and other resources efficiently.

Survivability requirement specified by two fundamental requirements, establishing a connection between nodes at any time and guarantees continuous connection until a specific amount of data is completely transferred between two nodes [6]. Essential service requirements to keep up routing survivability For MANET are Integrity, confidentiality and authenticity principles. Protection of wireless communication at the physical layer and access control of each node is important for routing survivability [7].

A number of researchers [7-9] agreed about four survivability requirements for MANET: 1) load balancing between nodes; 2) to be able to discover services and configure connection parameters; 3) to be able to adaptive node power to ensure uninterrupted services as long as possible; 4) efficient use of energy when the node is exposed to attack.

3. DoS MANET Attacks

DoS is one of the devastating attacks which aims to violate the availability of MANET, it increases its capacity causing only one hop communication and preventing packets to arrive to the destination node. DoS attacks intend to violate the important survivability goal, availability. It is trying to disrupt MANET from continuing to provide services in a timely manner. Most of DoS attacks in MANET are attacking routing protocols in the network layer to achieve their goals: Absorption of network traffic, inserts itself between source and destination to control the network traffic flow.

Flooding Attack: This type of attack intends to consumption node resources significantly such as bandwidth and battery power, or disrupting the normal routing operation. Flooding attack can happened when a malicious node send a large number of Route-Request (RREQ) packets in a very short time to a none existent node and there will not be Route-Replay (RREP), so the (RREQs) will flood network. As a result the throughput decreasing significantly; or flooding the destination node with a large number of unnecessary packets, it cannot receive all packets therefore all packets will discard [10].

Wormhole Attack: This type of attack occur when an attacker tunnel the routing control message to another location using a high speed communication link to prevent the completion of routing discovery process. This attack is one of the most sever attacks encounter mobile ad hoc network, it can overcome the authenticity and confidentiality communication, this shows the seriousness of this attack.

Rushing Attack: Rushing attack is a special type of wormhole attack occurred if a fast channel dedicated between two wormhole nodes, it intend to attack on-demand routing protocols that use duplicate suppression at each node used by many wireless routing protocols. In rushing attack, the adversary node floods the RREQ packet faster than other nodes which make legitimate nodes receive the same packets twice it assume these legitimate RREQs are duplicate packets and it is simply discard. Source node considers that adversary node as normal intermediate node, therefore source node could not find the route path that do not including adversary node.

The most dangerous attacks against MANET routing protocols which results in Denial of service is rushing attack, because the shared high speed transmission path between two end wormhole nodes which called rushing attack prevent current secure routing protocols from discovering route more than two hops. The other thing makes rushing attack dangerous that it can perform also by week attackers.

Black Hole Attack: In this attack, the malicious node pretend that it is a legitimate node and it has a valid route to the destination node, therefore the source node will select it, although it does not has a valid route. Black hole attack intends to damage or prevent some of forwarded packets while leaving some packets undamaged.

Byzantine Attack: A malicious intermediate nodes works alone or colluding to perform routing problems such as selecting a non-optimal path to forwarding packets or creating routing loops for packets or dropping a selected packets which results in significantly of throughput degradation or routing disruption.

4. Classification of DoS Attacks

Many researchers have done to define and classify DoS attacks [11,12] to help for more analysis and investigation about it. Attacks on MANETs are categorized into passive attacks and active attacks depending on the target of the attack.

Another classification of attacks by [4] as external attacks and internal attacks, external attacks is the attacks comes from outside, while internal attacks from inside the networks. Attacks can be classified according to the OSI model.

Most of research groups classify attacks in two main groups, but we suggested a new line of classification considering the behavior of different attacks appeared in the recent researches as shown in **Figure 1**.

4.1. Active Attacks

Active attack intends to objection the normal activity by fabrication, interruption or modification [3]. Active attacks are more dangerous because it is preventing

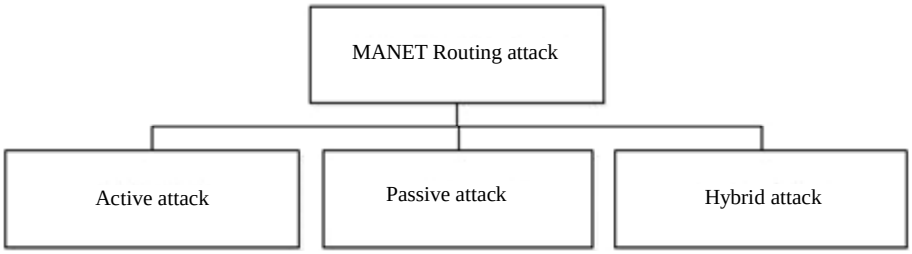

Figure 1. The new classification line of MANET attacks.

MANET from providing its service, but it is easy to detect than the passive attacks. [11] presented a common DoS attacks on network layer and they have more effects on MANET than other attacks, these attacks are wormhole attack, black hole attack and gray-hole attack. A wormhole attack is happen when two malicious nodes connected through a high speed link and cooperative with each other forming one of the very dangerous tunneling attacks. The two malicious nodes are placed at a very powerful position in the network, therefore most of the traffic in the network is going through these nodes, so they falsify the route length and drop delivered messages. Wormhole is invisible in the route, so it is difficult to discover.

Black hole exploit the principle of selecting shortest path by routing protocol to introduce itself that it has a shortest path after it selected by the source node to send packets it drop them. Most of the proposed approaches to detect or prevent black hole are analyzing or calculating distance between source and destination to discover malicious nodes; or using more than one node to receive RREP; or using common neighbor listening [13].

Gray-hole attack sometimes acting as normal node and sometimes acting as malicious node, due to this behavior it is difficult to deal with and it is degrades the networks performance.

All approaches and mechanisms proposed to detect or prevent gray hole attacks are uses different analytical process to analyze acknowledgement and RREP that received from the destination to discover if there is any suspicious behavior of malicious nodes in the network.

4.2. Passive Attacks

A passive attack intends to obtain data transmitted without objection the communication or altering data packets by electronic eavesdropping (wiretapping), traffic analysis, or monitoring data traffic. In eavesdropping attacker try to obtain sensitive information such as public and private key or location information. Detection of passive attacks is not easy because the normal operations of data routing are not affected. The useful way to protect data against passive attack is to encrypt transmitted data using encryption mechanism to prevent attacker from getting useful information from it.

4.3. Hybrid Attacks

Some attacks that are classified as active, sometime works as passive, and vice versa, for example DoS attacks are classify as active attacks, but [12] found that some DoS attacks are passive attacks; black hole considered as active as well as passive attacks. Some other passive attacks works as active attack by discards packets silently or hiding partial routing information; so these attacks are classified as hybrid effect.

5. MANET Routing Survivability Initiatives

Mobile ad hoc networks are susceptible to a broad range of attacks and intrusions; Denial of Services attack occurs when ad hoc routing function is completely subjected to vandalism, it is one of the affected attacks to the MANET operations. Many initiatives have proposed to keep MANET free of DoS attacks and survive in adversarial environments, in this section the most important and valuable of these initiatives and has a good improvement to MANET availability will be discussed. By studying initiatives we found that it's followed different ways to achieve MANET survivability. On these bases we classified it into three main groups: Initiatives based on authentication, Initiatives based on path selection, and Initiatives based on attack location and detection, as described in **Figure 2**.

5.1. Initiatives Based on Authentication

Impersonation is one of the main problems in MANET that results is many communication problems and violate security and survivability properties, so authentication is one of the prime rib of the survivable system. The main goals of discussed techniques and approaches are using authentication techniques to support MANET survivability.

The first technique proposed to improve MANET survivability using authentication is the Techniques for Intrusion-resistant Ad Hoc Routing Algorithms (TIARA), it is a group of techniques work together to mitigate the impact of (DoS) attacks, also it can defend against route

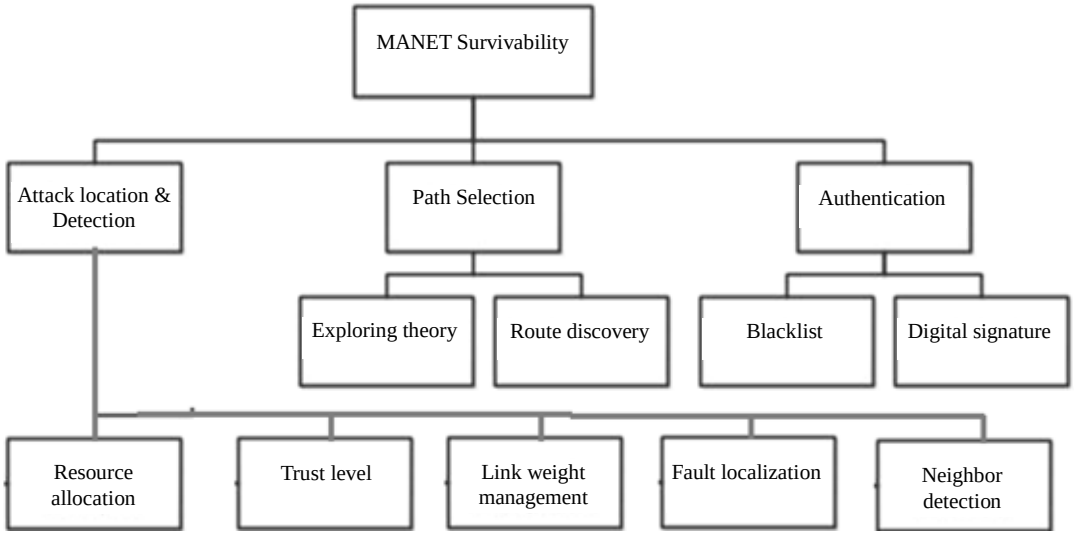

Figure 2. Classification of MANET survivable techniques.

hijacking, flow disruption, and resource depletion attacks. TIARA based on a five design techniques, flow-based route access control (FRAC), flow monitoring, source-initiated router switching, fast authentication, and referral based resource allocation. For countering different type of threats, TIARA uses a set of mentioned techniques [14].

Flow-based Route Access Control (FRAC), this technique makes a control to a flow sequence of packets between the source and destination node. Each intermediate node should retain a general route policy for the whole network to define authorized flow of each intermediate node, authorized flows are only forwarded. The routing algorithm should be modified in order to implement FRAC with the existing routing protocols and to ensure that the packet forwarding decisions are made by the flow-id. Because of the most of current routing algorithm are unable to maintain more than one route, so multipath routing enable to discover and maintain all legitimate routes. On-demand routing algorithm should be modified to enable them to multipath routing information. Routing algorithm should be modified to incorporate multi-path routing. This technique used to detect path failure and inform source node about the detected failure, so that the source node can select another route to complete sending the rest of the packets. In order to perform flow monitoring, the flow status massage is encrypted by digital signature and sent by the routing function, from the source and the destination node including sequence number. Source node uses this technique to determine the best route to select when there are multiple routes exist between source and destination node. To enable intermediate node select the best route, the source label each packet with information of the best path. To implement this technique, intermediate node should be implemented with technique to read the label of the packet. Fast authentication is a light mechanism used instead of traditional packet authentication techniques to authenticate data packets. Such a mechanism based on the notion of label of a packet, each packet place with path label at a specific secret location and it moves to each node in the route. To avoid traffic analysis attack, fast authentication should change the secret location in the packet periodically. Resource depletion attack will be severe when two colluding attacker cooperating with each other through a direct link. To defend against this attack, each node should define initially the threshold of the maximum required number of network resource. If there are more required to additional resources referral based resource allocation can grantee the required resource if source node present referrals from other trusted node. These techniques are incorporated in the existing routing protocols for building intrusion tolerant routing Ad Hoc networks that can provide services at a suitable level in the presence of mentioned DoS attacks.

Another algorithm Works on the principle of authenticcation is the Best effort Fault Tolerant Routing algorithm (BFTR), it is a source routing algorithm developed by [15]. It intends to deliver packets in high ratio regardless of the presence of adversaries. It selects the most shortest and feasible path by using statistics and DSR flooding, if the path is becoming infeasible at any time, the algorithm will discard it. The criterion used by BFTR to select path is end-to-end performance measured using the data packet transmission ratio and acknowledgement. BFTR can ensure correct end-to-end packet delivery under different misbehaving attacks, dropping, corruption, misrouting, tampering, delaying, fabrication and replaying.

Based on end-to-end verification and path diversity, an

approach is presented to increase reliability and survivability of MANET. The approach is applied to Secure routing though Diversity and Verification (SRDV) protocol. Path diversity is a solution to both problem malicious behavior and shortage of connection. The proposed protocol uses digital signature and hash chain to perform secure communications. The idea of SRDV protocol is using some security primitives such as digital certificate to get authentication between source node and target, it detects attack by using end-to-end delay and feedback on the number of data packet [16]. The proposed protocol uses the combination of techniques: path diversity, end-to-end verification, hash chain and digital signature to defend against individual or colluding attackers.

Discussion

Previous discussed initiatives are using authentication techniques such as: end-to-end verification, acknowledgement, digital signature, and hash chain to support MANET routing survivability, but their performance are affected by some deficiencies; for instance, TIARA efficiency reduced is in some cases. In the path failure a compromised node could not be specifically identified and the flow status message can cause additional traffic. Finally, the author did not explain precisely the way of implementing TIARA with routing protocols or how to make changes to the routing algorithm in order to incurporate the technique with the current on-demand routing protocols such as AODV or DSR. Also, BFTR will not perform well when misbehaving nodes are increased and when network become heavy loaded. Therefore, there is a need in another algorithm to handle much more misbehaving nodes.

5.2. Initiatives Based on Path Selection

If an attacker or malicious node placed itself in a path between source and destination node, that path will become un-selectable when source node initiates a routing discovery process in order to avoid transmission problems. Techniques uses path selection to support MANET survivability have discussed in more details.

Byzantine attacks such as a wormhole, black-hole, flood-rushing and overlay network wormhole can be mitigated by another technique called On the Survivability of Routing Protocols in Ad Hoc Wireless Networks (ODSBR). It is an on-demand source routing protocol provides service in the presence of Byzantine attacks and it uses all available paths to deliver data to the destination node. The secure on-demand routing protocols are assumes that only authenticated nodes can be trusted are always fails to standoff such attack. ODSBR assumes that source and destination are only full trusted and other nodes can be compromised [17]. The protocol work using three phases, each phase performs a specific task, these phases are:

Routing discovery: This phase based on a metric used to capture the history of link weight to locate the reliability of the link, where the high weights denote low reliability. Each node in the network maintains a list of link weight, when fault detected the list updated dynamically. In the route discovery, the source node always finds the lowest link weight using double flooding, per node flooding verification, and forwarding rules. The link with high weight will not be selected until it gets free of faults.

Fault localization: A secure acknowledgment sent from intermediate node along the route to verify that packets have successfully delivered to the destination without corruption. Adaptive Probing Technique (APT) used by the source node to identify faulty link and increase the link weight in the list. Link with highest weight will be avoided in the next routing selection. In APT the intermediate node sends a secure acknowledgement back to the source node beeline the route; it is a cryptographic proof for packet successfully delivering. The structure of APT helps to localize the malicious node when it causes a fault.

Link weight management: The weight of faulty links increased until sufficient numbers of acknowledgments are received, If the weight of the link is increased due to faults, this weight is maintained until destination sends enough number of correct acknowledgments [17,18].

A new strategy based on AODV protocol proposed by [19] to mitigate the impact of link-discontinuing and reduce packet delay. The idea of proposed mechanism Survivable Routing Strategy (SRS) is used optimal exploring theory to find a new available next hop to establish a new connection if the next hop was malicious.

When establishing a new connection through an optimal exploring equation there is a node shared in both old and new link called survivable node it becomes the current node where the route to the destination node through the new link will restart from it. The vector angle between survivable node and destination will be calculated by the proposed new strategy. Vertex angle is used to increase the successful exploring probability. The proposed strategy significantly improves the performance of MANET; it increases successfully the delivery route, lower overhead, reduction end-to-end delay than traditional AODV and improves survivability of MANET. To support MANET routing survivability through a combination of preventive, reactive, and tolerant defense lines, each defense line provide security criteria and fuzzy logic correlate between them, a new scheme have proposed by [20]. The proposed scheme based on fuzzy logic to reduce routing protocol security limitations to select the most survival path. Different criteria such as

path characteristics and interaction with the data link layer are used for better path selection. To achieve path selection using fuzzy logic three phases will be involved data collection, fuzzy inference and adaptive path selection. In the first phase, check packet will collect data periodically to find node-disjoint multipath route between source and destination and collect information of the survivability level. The survivability level of each path will calculate by fuzzy logic in the fuzzy inference phase. The path with high survivability level will be selected in the path selection phase. In every time the most survival path will be selected if the path broken or if the new data collection phase occurs, this process make routing more responsive to network changes. Long-living path between source and destination is leading to MANET availability properties; it is required by many of MANET's applications today. Three different path selection algorithms have proposed by [21] to select the best path from a set of available paths. The proposed algorithms are takes into its account for selection decision the mobility-induced impact and path lifetime. The path will be selected if its Residual Path Lifetime (RPL) long or meat its requirement. Two of the three proposed algorithm needs to compute Full link Lifetime (FLL) statistics at each node until a sufficient number of statistics collected. FLL statistics is the time length beacon takes from node A to node B, FLL histogram obtained by repeating by repeating the process. To evaluate the ability of the proposed algorithms to find the best path, two performance metrics have introduces, the first performance metric evaluate the ability of the algorithm to meet the RPL requirement. The second one evaluates the ability of the algorithm to select the path with the longest residual lifetime. The limitation of the proposed algorithms is that they are perform better in a high mobility environment only, but in low mobility environment the performance degrades significantly.

Discussion

Current multipath routing protocols has some limitations, it does not take into account different selection parameters. It considers only two or three number of selection criteria and a few of them considers about security issue. Due to MANET characteristics depending on security criteria only, it is not enough to supporting survivability using path selection. ODSBR has some overhead represented in the presence of Byzantine attacks it requires bidirectional flooding to guarantee correct route. When comparing to AODV, ODSBR transmit more packets than AODV which it is transmitted route request and route replay while AODV transmit only route request. When the number of adversaries increasing, the overhead of ODSBR increase while the overhead of AODV decrease. Also, the performance decrease when need to handle with a large number of faulty links.

5.3. Initiatives Based on Attack Detection & Location

Detection and localization of adversarial nodes in the network are the important aspects in the most of the survivability initiatives. After detection of malicious node or suspicious activity in MANET, it is important to locate it to avoid the path contains that suspicious activity. The following discussed initiatives are using detection and location to support MANET routing survivability. There are two effective methods have done to prevent rushing attacks, one have done in 2003 by [22] and the other one in 2011 by Al-shahrani [23]. A component based on route discovery called Rushing Attack Prevention (RAP) proposed to detect rushing attack [22]. It can be integrated with the existing on-demand routing protocols (AODV and DSR). The proposed prevention technique RAP consist of three techniques works together to defend against rushing attack, these techniques are:

1) Secure Neighbor Detection (SND);
2) Secure Route Delegation (SRD);
3) Randomized Route Request Forwarding (RRRF).

This technique discussed and solved a special type of rushing attack when the attacker forwards a route request beyond the normal range of transmission using higher power level; in this case the first technique of the presented protocol, SND allows both sender and target nodes to verify that they are in the normal range. The on-demand routing protocols included implicitly a neighbor detection but it does not preventing attacker from simply replaying it. SND prevent attacker from introducing any nodes that are out of normal transmission range from introducing themselves as neighbors and preventing attacker from claiming that it is a neighbor. SRD technique used to verify that SND steps performed between adjacent pairs of nodes. The third technique RRRF used to complement the two mentioned techniques to completely prevent rushing attack is Randomized Message Forwarding which preventing attacker from dominate all routes. New approaches for wireless ad hoc network have proposed to become more tolerant against flooding attacks and other intrusions launched by attacker. The approach depends on taking advantage of existing application capability to handle intruders. The approach suggested a Resource Allocation Mechanism (RAM) implemented with the wireless router through a suggested component [24]. The approach assumes that MANET is divided into two virtual sets, resource domain and user domain. It is built of a multilevel of trust and network mechanism for resource recovery and allocation. Each activity in the network has a trust level assigned by resources. To maximize the use and minimize the cost,

applications can allocate resources using a distributed scheme and based on the activity and trust level. At each node only a portion of resources is allocated for each application. Each node maintains a firewall table, each table consist of a list of packets passing through it whether they delivered successfully or not. After handshake between source node and destination node the firewall table of each node updated automatically if packets delivery failed. The MANET is protected against flooding attack though a distributed firewall. The proposed scheme uses wireless ad hoc routing and wireless GRID computing and based on managing a multi trust levels in a real time it offers fault and intrusion tolerant services. In order to support MANET routing protocol survivability to mitigate different types of routing attacks including (DoS), Geng and Zou proposes a new routing mechanism based on Common Neighbor Listening (CNL). The mechanism assumes that in MANET any two different nodes have the same neighbor called common neighbor and changing of the neighbor not much. To evaluate nodes and classifies them whether they are malicious or legitimate, each node has a trust_value and maintains a list of trust_values of other nodes; this value increases quickly and decreases slowly depending on its behavior. The node which has bigger trust_value is the first one has a higher priority to listen. If the route to the destination is lost the common neighbor node search for another route to continue delivering the packets [25]. Al-Shahrani proposes two mechanisms to help MANET to survive in the presence of rushing attacks by reducing the overhead and delaying time in SDSR routing protocol. He supposes two problems countering SDSR and proposes their solutions. The first supposed problem is that there are three positions of attackers in the network causing rushing attack. The first problem, the impact of the attacker is differ depending on their position, if the attacker is near the source or destination, the impact will be highly harmful, otherwise the impact will reduced. In this case, Al-Shahrani proposes a solution called safe neighbor, this solution depend on blacklist technique, the source node sends request packet which the source and destination has the address of this packet, so neighbor node of the sender node which deliver the requested packet in a required time will be listed in a whitelist; if there is some delay the node will be listed in a gray list, otherwise it will be listed in a blacklist.

The second problem, if there are many senders node to many destinations node at the same time, this will lead to collision or significant delay then rushing attack. The suggested solution to solve this problem is a new algorithm to prevent nodes from holding more packets in its queue to prevent packet delay. The proposed algorithm will reduce time required by SDSR by half and reduce the overhead in the network [26].

Discussion

Detection and localization of malicious node and suspicious activities by previous discussed initiatives are implemented using different techniques: SND, SRD, RRRF, RAM, CNL, and blacklist.

Some shortages related to some proposed techniques; for RAP technique it is defends against special type of rushing attack as mentioned above; also it incurs higher overhead than other route discovery techniques, but it provides a usable route discovery than other do.

The mechanism proposed by Geng and Zou, has no overhead to the normal operation of MANET, but it has some deficiencies, if all the common neighbors are under the ***hold_value*** of being trusted then there will be no trusted route to the destination.

6. Discussion and Open Points

As we can see, all the presented initiatives are aimed to mitigate the impact of DoS attacks and keep MANET survivable and continue providing its services in the presence of attacks. All proposed techniques are implemented in the existing routing protocols and consist of set of techniques works together, each technique perform specific function. By studying these initiatives we found that all proposed solutions are based on one or more of previous discussed techniques, these techniques are: authentication, resource allocation, neighbor detection, route discovery, fault localization, link weight management, trust level, exploring theory, and blacklist technique. All mentioned techniques can be classified into three main categories: authentication, path selection, and attack location and detection.

All proposed approaches and techniques are aims to mitigate the impact of DoS attacks or detecting it, it has some deficiencies which make them fail in some cases such as in strong and colluding attacks, or when MANET exposed to heavy load, which make MANET still in problem. **Table 1** summarizes all previous discussed techniques. **Table 2** summarizes the above-mentioned approaches and which attacks defend against.

All discussed initiatives are using a set of existing techniques to perform survivability goals for MANET which causes some of main deficiencies. Deficiencies can be summarized for more investigation as open points:

Overhead reduction: Most initiatives cause additional overhead in MANET because of using a set of existing techniques. Reducing of overhead can be accessed by efficient use of these techniques depending on current MANET status.

Security features: Most of proposed techniques are implemented with AODV routing protocols which is not supporting security features such as SAODV. Taking the

Table 1. Summarize of MANET survivability initiatives.

Technique	Attack	Approach	Implementation	Deficiencies	Date
TIARA	DoS	Based on set of techniques: flow-based route access control (FRAC), flow monitoring, source-initiated router switching, fast authentication, referral based resource allocation	Implemented with the existing routing protocol.	1. In the path failure a compromised node could not be identified. 2. Flow status message can cause additional traffic. 3. Implementation did not explained by author.	2003
RAP	DoS (rushing attack)	Based on three technique: 1. Secure neighbor detection, 2. Secure route delegation 3. Randomized route request forwarding	Integrated with AODV or DSR.	1. It defends against special type of rushing attack. 2. It incurs higher overhead than other route discovery.	2003
BFTR	Dropping, corruption, misrouting, tampering, delaying, fabrication and replaying	The criterion used is: end-to-end performance measured using the data packet transmission ratio and acknowledgement	Undefined	It will not perform well when misbehaving nodes are increased and when network become heavy loaded	2004
BA	Flooding attacks	1. Suggest a resource allocation mechanism (RAM): depends on taking advantage of existing application capability to handle intruders. 2. Uses wireless ad hoc routing and wireless GRID computing and based on managing a multi trust levels in a real time	(RAM) implemented with the wireless router through a suggested component.	Undefined	2005
Mechanism by Geng	DoS	1. New routing mechanism based on common neighbor listening. 2. Each node has a trust_ value increases quickly and decreases slowly depending on its behavior. 3. Bigger trust_value = higher priority to listen.	Undefined	If all the common neighbors are under the threshold_value of being trusted then there will be no trusted route to the destination.	2006
Scheme by Lima	DoS	1. Residual path lifetime. 2. Full link lifetime.	Implemented in nodes.	In low mobility environment the performance degrades significantly.	2006
Approach by Dabideen	DoS	1. Based on end-to-end verification and path diversity. 2. Uses digital signature and hash chain. 3. Detects attack by using end-to-end delay and feedback on the number of data packet.	Applied to secure routing though diversity and verification (SRDV) protocol.	Undefined	2009
Strategy by Dan-Yang	1. DoS 2. Link-discontinuing and reduce packet delay	1. Proposes mechanism survivable routing strategy (SRS). 2. Uses optimal exploring theory. 3. SRS calculate the vector angle between survivable node and destination.	Based on AODV protocol	Consumes more of CPU times.	2011
Mechanisms by Al-Shahrani	DoS (Rushing attack)	Two solutions proposed: 1. A neighbor safe solution based on blacklist technique. 2. A new algorithm.	Based on SDSR protocol	Limited to solve SDSR problems.	2011

security into account can provide better performance for used techniques.

Hybrid attacks consideration: as discussed in Section 4.3, there are passive attacks sometimes work as active attacks, for better support to MANET survivability, this type of attack should be taken into consideration in the future survivability solutions.

7. Conclusion

Because of the widespread use of MANET applications

Table 2. Approaches and attacks.

Approach	DoS attack							
	Rushing	Flooding	Wormhole	Blackhole	Byzantine	Route hijacking	Flow disruption	Resource depletion
TIARA						✓	✓	✓
RAP	✓							
BFTR			✓	✓			✓	
BA					✓			
Scheme by Lima	✓			✓				
Mechanism by Geng			✓			✓		
Approach by Dabideen			✓	✓				
Strategy by Dan-Yang						✓	✓	
Mechanisms by Al-Shahrani	✓	✓						

today's, different types of attacks have developed as well. The traditional defenses techniques are not enough to defend against all types of attacks mentioned above, so this survey have discussed a group of techniques that can help MANET to defend against these new types of attacks. We have discussed the most important and valuable initiatives techniques and approaches that proposed to keep MANET survive and provide its services in the existence of active attacks, also we highlight the deficiencies of these initiatives and attacks which it can defend against.

REFERENCES

[1] A. K. Rai, R. R. Tewari and S. K. Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication," *International Journal of Computer Science and Security*, Vol. 4, No. 3, 2010, pp. 265-274.

[2] H. L. Nguyen and U. T. Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks," *Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies*, 23-29 April 2006, 149 p.

[3] B. Wu, J. M. Chen, J. Wu and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," *Wireless/Mobile Network Security*, Springer, Berlin, 2007, pp. 103-135.

[4] V. Gokhale, S. K. Ghosh, *et al*., "Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks," *Security of Self-Organizing Networks*, Auerbach Publications: MANET, WSN, WMN, VANET, 2010, p. 195.

[5] Y.-C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," *IEEE Security & Privacy*, Vol. 2, No. 3, 2004, pp. 28-39. doi:10.1109/MSP.2004.1

[6] K. Paul, R. R. Choudhuri and S. Bandyopadhyay, "Survivability Analysis of Ad Hoc Wireless Network Architecture," *Mobile and Wireless Communications Networks*, Springer, Berlin, pp. 31-46.

[7] M. N. Lima, A. L. dos Santos and G. Pujolle, "A Survey of Survivability in Mobile Ad Hoc Networks," *IEEE Communications Surveys & Tutorials*, Vol. 11, No. 1, 2009, pp. 66-77.

[8] Z. Yanjun, "A Framework of Survivability Requirement Specification for Critical Information Systems," 43*rd Hawaii International Conference on System Sciences*, Piscataway, 2010.

[9] M. N. Lima, H. W. da Silva, *et al*., "Requirements for Survivable Routing in MANETs," 3*rd International Symposium on Wireless Pervasive Computing*, 7-9 May 2008, pp. 441-445. doi:10.1109/ISWPC.2008.4556246

[10] Y.-C. Hu, A. Perrig and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Wireless Networks*, Vol. 11, No. 1-2, 2005, pp. 21-38. doi:10.1007/s11276-004-4744-y

[11] A. A. Cardenas and N. Benammar, G. Papageorgiou and J. S. Baras, "Cross-Layered Security Analysis of Wireless Ad Hoc Networks," DTIC Document.

[12] A. K. Jain and V. Tokekar, "Classification of Denial of Service Attacks in Mobile Ad Hoc Networks," *International Conference on Computational Intelligence and Communication Networks*, Gwalior, 7-9 October 2011, pp. 256-261. doi:10.1109/CICN.2011.51

[13] R. C. Linger, N. R. Mead, *et al*., "Requirements Definition for Survivable Network Systems," *Proceedings of the 3rd International Conference on Requirements Engineering*, Washington DC, 1998, pp. 14-23.

[14] R. Ramanujan, S. Kudige and T. Nguyen, "Techniques for Intrusion-Resistant Ad Hoc Routing Algorithms (Tiara)," *DARPA Information Survivability Conference and Exposition IEEE Computer Society*, Los Alamitos, 2003, pp. 98-100.

[15] B. Awerbuch, R. Curtmola, *et al*., "On the Survivability of Routing Protocols in Ad Hoc Wireless Networks," 1*st International Conference on Security and Privacy for Emerging Areas in Communications Networks*, 5-9 Sep-

tember 2005, pp. 327-338.

[16] S. Dabideen, B. R. Smith and J. J. Garcia-Luna-Aceves, "An End-to-End Solution for Secure and Survivable Routing in MANETs," 7*th International Workshop on Design of Reliable Communication Networks*, Washington DC, 25-28 October 2009, PP. 183-190.

[17] R. H. Jhaveri, S. J. Patel, *et al*., "DoS Attacks in Mobile Ad Hoc Networks: A Survey," 2*nd International Conference on Advanced Computing & Communication Technologies*, 2012.

[18] B. Awerbuch, D. Holmer, C. Nita-Rotaru and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," *ACM Workshop on Wireless Security*, 2002.

[19] D.-Y. Qin, L. Ma, X.-J. Sha and Y.-B. Xu, "An Effective Survivable Routing Strategy for MANET," *Tamkang Journal of Science and Engineering*, Vol. 14, No. 1, 2011, pp. 71-80.

[20] M. N. Lima, H. W. da Silva, *et al*., "Survival Multipath Routing for MANETs," *IEEE of Network Operations and Management Symposium*, Salvador, 7-11 April 2008, pp. 425-432. doi:10.1109/NOMS.2008.4575164

[21] E. Y. Hua and Z. J. Haas, "Path Selection Algorithms in Homogeneous Mobile Ad Hoc Networks," *Proceedings of the* 2006 *International Conference on Wireless Communications and Mobile Computing*, New York, 2006, pp. 275-280.

[22] Y.-C. Hu, A. Perrig, *et al*., "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," *Proceedings of the* 2*nd ACM Workshop on Wireless Security*, San Diego, 2003, pp. 30-40.

[23] A. S. Al Shahrani, "Rushing Attack in Mobile Ad Hoc Networks," 3*rd International Conference on Intelligent Networking and Collaborative Systems*, Fukuoka, 30 November-2 December 2011, pp. 752-758. doi:10.1109/INCoS.2011.145

[24] N. A. Boudriga and M. S. Obaidat, "Fault and Intrusion Tolerance in Wireless Ad Hoc Networks," *IEEE of Wireless Communications and Networking Conference*, Vol. 4, 2005, pp. 2281-2286. doi:10.1109/WCNC.2005.1424871

[25] P. Geng and C. Zou, "Routing Attacks and Solutions in Mobile Ad hoc Networks," *International Conference on Communication Technology*, Guilin, 27-30 November 2006, pp. 1-4.

[26] Y. Xue and K. Nahrstedt, "Providing Fault-Tolerant Ad Hoc Routing Service in Adversarial Environments," *Wireless Personal Communications*: *An International Journal*, Vol. 29, No. 3-4, 2004, pp. 367-388. doi:10.1023/B:WIRE.0000047071.75971.cd

