An Experimental Analysis on Various Techniques for Malicious node Detection in MANET

Chetan S Arage, K. V. V. Satyanarayana

Abstract*: Mobile ad hoc networks (MANETs) are a subclass of wireless ad hoc networks having exceptional characteristics of dynamic system topology and moving nodes. MANETs are infrastructure-less, self arranging networks intended to support mobility. Because of these attributes, there is need of separate routing protocols for MANET. The advantages such as non-limited versatility, simple organization attributes of MANETs make them exceptionally important and very reasonable mainly for crisis situations and military applications. Within the sight of malevolent nodes, this prerequisite may lead to genuine security threats; for example, such nodes may disturb the routing process. In this specific circumstance, avoiding or identifying malicious nodes launching grayhole or collaborative blackhole attacks is a challenge. This paper is focuses on surveying and a reviewing of MANET security attacks and approaches to defend from vulnerabilities. The routing protocol mainly concerned in this approach is Dynamic Source Routing Protocol (DSR). The schemes like Watchdog, TWOACK, AACK, EAACK and CBDS have been used for detection of malicious nodes in MANET. Our research aim is to identify current trends, open challenges and future research directions in the deployment of MANET by considering the malicious node detection scheme. In order to bridge the research gap in terms of performance, detection rate and overhead; also to overcome the challenges of existing security issues regarding MANET. The aim is to propose an improved cooperative bait detection scheme (ICBDS) to detect malicious node maintaining minimal overhead.

Keywords* : Watchdog, Mobile Adhoc NETwork (MANET), Security, Enhanced Adaptive ACKnowledgement (AACK,EAACK).

I. INTRODUCTION

Exploitation of network due to malicious node attack disrupts the reputation, trust and confidentiality of using total network. Further it may lead to trust and privacy issues and can prevent the users using the concept of MANET. There is a chance of new flaws because of development of new code or software in today's life.

1.1 Security attacks categorization in MANET

The approaches like EAACK, Watchdog, TWOACK are prone to false alarms and false detections. In such kind of situation MANET will collapse, no matter which security measures and solutions are being used. Thus, it is required to re-modify and preplan the whole network which eventually may lead to high routing overhead in terms of cost. Although there are a lot of enhancement in technology of MANET, but it is vulnerable to many existing and new security attacks and so it needs to be addressed. Passive attacks include the release of message contents and traffic analysis while active attacks can be divided into, masquerade; reply; modification of messages and denial of service.

Following major attacks can be challenge to the working of MANET [25].

1.1.1. Denial of service attack (DoS)

This kind of attack is especially on availability and it is executed by making the resource unavailable for authorized users. This attack works by sending the jamming signal into the communication channel so preventing legal users from accessing the network and its resources. Attacker eventually sends huge amount of garbage traffic to a particular node and makes disruption in routing process. Attacker may also drop all the packets forwarded to it and makes traffic information unavailable for other nodes in network.

1.1.2. Distributed denial of service attack (DDoS)

In this attack instead of single attacker, multiple stations acts as an attacker to overwhelm the node.

1.1.3. Tampering with the information

In such attack, an attacker may tamper the information like current location, routing packets information to disturb the MANET functionality.

1.1.4. ID disclosure

This attack involves disclosing and stealing the identities of other nodes and uses this identification for further attacks on MANET.

1.1.5. Wormhole attack

It involves two or more than two malicious nodes and packets from one end

Revised Manuscript Received on July 25, 2019.

Chetan S Arage, K. V. V. Satyanarayana, Department of Computer Science Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur – 522502,Andhra Pradesh, India;chetan.arage@gmail.com , kopparti@kluniversity.in

of malevolent node is tunneled to other malicious node .These data packets are further broadcasted. Thus it disturbs the routing in case of multicast and broadcast.

1.1.6. Black hole attack

In this kind of attack, malicious node attracts other node by sending them information that it has shortest path to the destination and in such way instead of forwarding the packets to the destination, it simply drops all packets.

1.1.7. Spoofing attack

Malicious node pretends to be a legal node for the purpose of stealing sensitive and private information for getting privileges.

1.1.8. Alternation attack

This attack includes delaying of transmission of data, replaying the earlier transmitted data or modifying the received data packets.

Attacks on MANET can be categorized on the basis of various attributes like "internal vs external" and "active vs passive attacks" on security parameters like availability, integrity, confidentiality and authenticity as shown in table1 below.

Sr No	Attack Name	Internal	External	Integrity Infringement	Confidentiality	Availability	Attack on Authenticity	Active	Passive
1	ID Disclosure	Y	Y		Y				Y
2	Misconfiguration	Y	Y		Y		Y	Y	
3	Worm Spreading	Y		Y	Y	Y		Y	
4	Brute force	Y	Y		Y		Y	Y	
5	Man in middle	Y		Y	Y	Y		Y	
6	DoS	Y	Y			Y		Y	
7	DDoS	Y	Y			Y		Y	
8	Blackhole	Y				Y		Y	
9	Warmhole	Y			Y	Y		Y	Y
10	Session Hijacking	Y	Y		Y		Y	Y	Y

Table 1 – Security attack categorization in MANET

II. LITERATURE REVIEW

Over the recent years, many review articles have been published on malicious node detection in MANET. A study of various recently Intrusion detection System in MANET and different classification of such approaches employed have been presented in [1-3],[17-25].

Following are the major approaches for malicious node detection in MANET:-

2.1 Dynamic Source Routing (DSR)

DSR is on demand source routing protocol. In this, route path are discovered at the time source send packet to destination node for which it has no path. Dynamic Source Routing has two phases

a) Route discovery
b) Route Maintenance

At first, source node initiates a route discovery by broadcasting a ROUTE REQUEST packet to its neighbors that contains destination address. In turn, neighbors append their own addresses to ROUTE REQUEST packet and rebroadcast it. This process is followed until packet reaches destination node. Destination node send back ROUTE REPLY packet back to the source node informing the discovered route. If there are multiple paths received by source node then DSR caches these routes in route cache for future use.

In second phase DSR handles link breaks. A link break occurs because of two nodes on a path are no longer in communication range. In link break case, intermediate node sends back a message to the source notifying the same issue. The source node must try another path or follow route discovery if it does not have another one.

2.2 Watchdog and Pathrater

There are two techniques that improve throughput in an ad hoc network in the presence of nodes willing to forward packet but fail to do so.

Watchdog identifies misbehaving nodes and Pathrater helps routing protocols to avoid malicious nodes. For example- Dynamic Source Routing.

Watch dog method detects malicious node. The watchdog technique is a strategy proposed before in different approaches that distinguishes misbehaving nodes acting alone by maintaining a buffer that contains as of recently sent packets. At the point when a node forwards a packet, it's watchdog guarantees that the next node in the path also forwards the packet. The watchdog does this by hearing all nodes promiscuously. In the event that the neighbor node does not

forward the packet, it is named as misbehaving. In this approach, each packet that is overheard by the watchdog is compared with the packet in the buffer to check whether there is a match. A match affirms that the packet has been effectively conveyed and it is expelled from the buffer. If a packet has remained in the buffer exceeds the timeout period, a failure counter for the node in charge of forwarding the packet is augmented. If this counter exceeds a predetermined threshold, the node is named as malicious and the network is informed accordingly by a message sent by the node that recognizes the issue. Following figure describes the working of Watchdog.

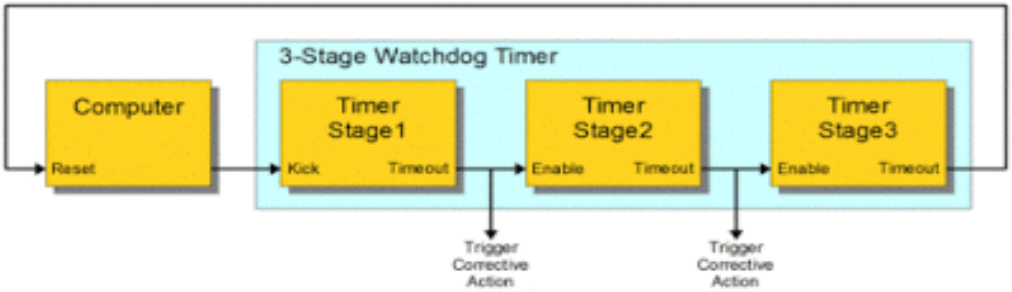

Figure 1- Watchdog Method

Assume that there exists a path from node S to D through A,B,C. Node A is not able to transmit all the way to node C but it can listen in on node B's communication .Thus whenever A forward a packet to C through B , it can often tell if B has tampered with the payload / header or not.

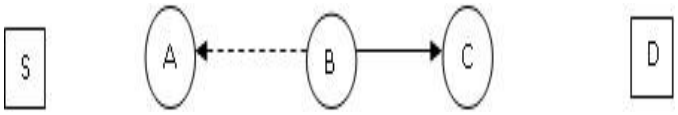

Figure 2- Node A can tell regarding tampering of data at Node B

For Watchdog method to work properly, it must know where a packet should be in two hops. Watchdog has this required information because of DSR and it works best on top of source routing protocol [3].

Advantage of this method is in the case of extreme mobility watchdog can increase network throughput [4].

When any node in the network becomes well known to pathrater using route discovery process, pathrater assigns it neutral rating of 0.5. In the case of rating to be done by a node itself, it assigns with 1.0.This guarantees that when calculating path rates, if all remaining nodes are neutral node (rather than malicious node), pathrater picks shortest path for communication. Ratings of the nodes are incremented by 0.01 at periodic intervals of 200ms on all actively used paths. These are the paths on which node has sent packet within last periodic interval. A neutral node can attain maximum value of 0.8. In [4], it is proposed that rating value will be decremented by 0.05 in the case of link break and unreachable node. Pathrater does not modify ratings of the nodes which are inactive.

When pathrater learns that there is a malicious node on a path and it is not able to find path free of misbehaving nodes, it send a ROUTE REQUEST.

Disadvantage of watchdog and pathrater is due to mobility of nodes there is increase in the overhead transmission from the routing protocol's 12% to 24% as mentioned in [7].

Watchdog scheme fails to detect malicious nodes with presence of the following:-

i. Ambiguous collisions
ii. Receiver collisions
iii. Limited transmission power
iv. False misbehavior report
v. Collusion
vi. Partial dropping

2.3 TWOACK

2ACK scheme can be used as an add-on technique to routing protocols like DSR in MANET.

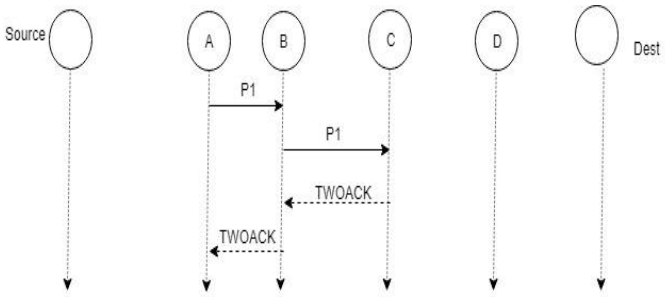

Figure 3- Each node is require sending back an acknowledgment packet to the node which is of distance two hops.

To overcome weaknesses of watchdog scheme, many researchers proposed new approaches to find the solution. The main aim is to resolve the receiver collision and limited transmission power problems faced by watchdog. TWOACK detects misbehaving link and malicious node by giving acknowledgement to every data packet transmitted over each three consecutive nodes from source node to destination node. Each node along the path is required to send back packet of acknowledgement to the node i.e. of distance two hops from it. TWOACK works best on the top of DSR [5].

In this work, If TWOACK packet is not received in time as threshold, the corresponding node is reported as malicious. The same procedure is

followed for every three consecutive nodes next on the path [5]. The advantage of this method is that it works successfully to solve the receiver collision and limited transmission problems faced by watchdog.

Disadvantages of TWOACK are as follows –
i) Acknowledgement procedure followed for every packet transmission process added a significant amount of routing overhead.
ii) TWOACK has to suffer from degradation of lifespan of entire network [3].
However, many research studies are working in energy harvesting to deal with such kind of situations [7-9].

2.4 AACK

The main purpose of Adaptive ACK scheme is to overcome the weaknesses of watchdog and to improve TWOACK scheme. AACK provides less routing overhead as compared to other. AACK works better than TWOACK and watchdog in video applications in presence of malicious node [15].

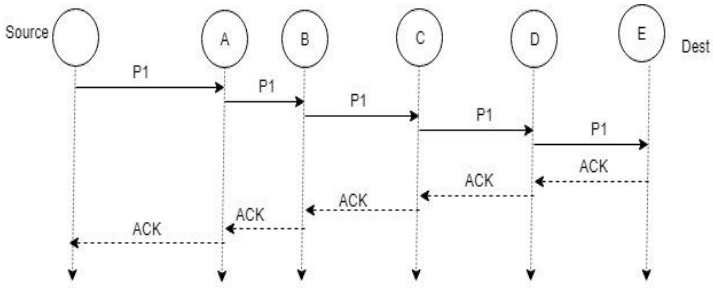

Figure 4- Working of ACK scheme

As shown in figure 4, Packet P1 is sent from source S to destination node E. Here destination node is required to send an acknowledgement back to the source. In timeout case source node S switch to TACK scheme which is identical to TWOACK by sending out TACK packet.
The advantage of this method is that AACK works as hybrid scheme which reduces the routing overhead of the network while disadvantage is that TWOACK and AACK fail to detect malicious node in the presence of false misbehavior report and forged acknowledgement.
Function of AACK and TWOACK depends on acknowledgement packet, so it is crucial to assure that the acknowledgement packets are valid and authentic [12]. To address this concern it is required to adapt digital signature for enhancement.

2.5 EAACK

In earlier approaches like TWOACK, AACK there is problem with validity and authenticity of acknowledgement packets. To overcome this scenario Enhanced Adaptive ACKnowledgement scheme adapt digital signature which are mainly divided into following two categories-
i) Digital signature with appendix e.g. DSA [10].
ii) Digital signature with message recovery e.g. RSA [11].

EAACK proposed in [3], designed to handle three weaknesses of watchdog scheme
i) False misbehavior
ii) Limited transmission power
iii) Receiver collision
These cases are described in figure 5,6,7.

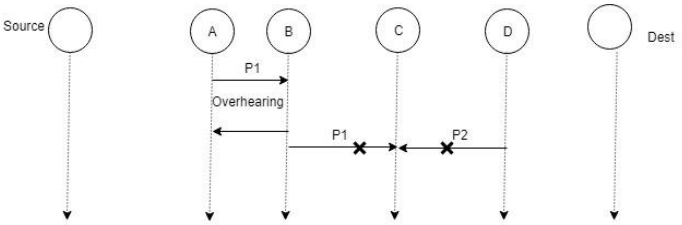

Figure 5 – Receiver collisions both nodes B and D are trying to send packet 1 and packet 2 respectively to node C at the same time.

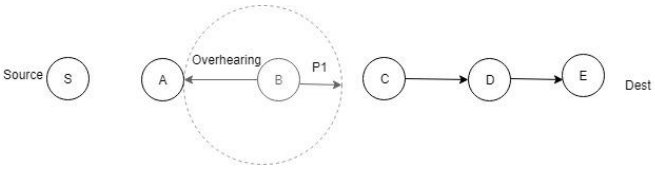

Figure 6 – Limited transmission power. Node B limits its transmission power so that [packet transmission can be overheard by node A but too much weak to reach node C.

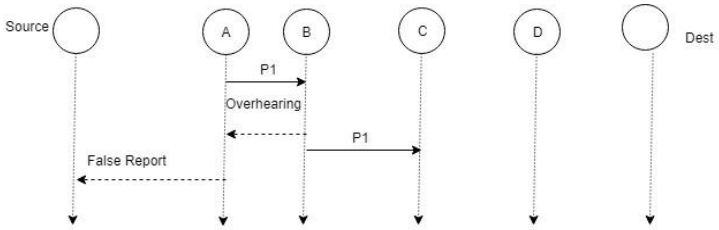

Figure 7 – False misbehavior report. Node A sends back misbehavior report to source node even though node B forwarded the packet to node C

TWOACK and AACK are vulnerable to false misbehavior report attack. Following are three major parts of EAACK
i) ACK
ii) Secure ACK (S-ACK)
iii) Misbehavior report authentication (MRA)

2.5.1 ACK

It is end to end acknowledgement scheme its aim is to reduce network overhead in the absence of network misbehavior. Within a predefined time threshold, if source node receives an acknowledgement packet then transmission is successful. Otherwise, source node switch to S-ACK mode by sending out S-ACK data packet to detect misbehaving node in the route.

2.5.2 S-ACK

It is improved version of TWOACK scheme [5]. The basic principle is to let every three consecutive nodes work in a group to

detect malicious nodes. From each three consecutive nodes, the third node is required to send S-ACK acknowledgement packet to the first node. The purpose behind this is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

If the first node does not receive acknowledgement packet within predefined time threshold then second and third node are reported as malicious. In TWOACK, source node immediately trust the misbehavior report but in EAACK requires the source node switch to MRA mode for making confirmation of misbehavior [5].

2.5.3 MRA

Watchdog fails to detect malicious nodes in case of false misbehavior report [3]. It can be generated by malicious attackers to falsely report innocent nodes as malicious. The main focus of this scheme is to authenticate whether destination node has received the reported missing packet through different path.

At the start of MRA mode, the source node searches its local knowledge base and finds for an alternate path to destination. If there is no path exists then the source node starts DSR ROUTE REQUEST to find another route. By adopting the alternate path to the destination node, we circumvent the misbehavior reporter node. Upon receiving MRA packet, destination node searches its local knowledge base and compares if reported packet was received. If it is received already then it is fine to conclude that this is false misbehavior report and the node which is responsible for generating this report is marked as malicious. Otherwise, misbehavior report is accepted [3].

In this scheme it is required that acknowledgement packet to be digitally signed before sending them out and verified until they are accepted. To address this concern DSA [10] and RSA [11] digital schemes have been already implemented.

2.6 Other attacks and approaches

In [17] authors have proposed that several multipath routing strategies are adopted Optimized Link State Routing (OLSR) protocol. Implementation of Multipoint Relay (MPR) nodes as a flooding mechanism for distributing control information has been included in MANET. In this method, the construction of multiple disjoint paths helps to increase resilience against network failures or malicious attacks. In OLSR networks, partial link-state information is generated and flooded exclusively by the MPRs. Therefore, the nodes only obtain a partial view of the network topology [17].In addition to this flooding disruption attacks may impact on either the selection of the MPRs or the propagation of traffic information. In [17] presented a strategy to compute multiple strictly disjoint paths between any two nodes in OLSR- based networks.

. In [18] authors have tried to resolve the attack issue through the design of dynamic source routing (DSR)-based routing approach, and that was termed as the cooperative bait detection scheme (CBDS). This has incorporated the benefits of both proactive as well as reactive defense models.. Finally, they have experimented with the simulation outcome, which have shown that in the presence of malicious-node attacks, the proposed CBDS performs well with respect to the ratio of packet delivery, end to end delay and routing overhead [18].This scheme is described in details along with modifications in[2].

In [19] authors have designed a new protocol that grants an effective route discovery model along with a competent Three Fish algorithm. The model has the basis of the understanding of nearby clusters and has effectively used the data for minimizing the overhead of routing using CEAACK in MANETs. The novel distributed routing protocol assures security, anonymity and high reliability of the established path in a hostile MANET environment. An enhanced three fish algorithm uses a unique key during the encryption and decryption process to ensure the safety of the data during a transmission [19].

In [20] authors have done the analysis on the behavior as well as the effect of JellyFish attack on TCP-based MANETs. Implementation and assessment all 3 jellyfish attack variants via the simulation method. Authors have proposed direct trust based detection algorithm which is useful to detect and remove Jellyfish node from active communication path. In this approach, each node uses locally calculated trust values which are collected over a time period to identify whether its neighbor node is a JF-attacker or not [20].

In [21] authors have investigated and proposed FbeeAdHoc security framework which is utilized the fuzzy set theory as well as digital signature. They have recommended using a toolbox TRUTIME with MATLAB for the purpose of network simulation. Outcomes of this simulation have shown that the developed model could counter the different types of attack and can outperforms when compared over ad hoc on-demand distance vector (AODV) [21].

In [22] it has been found that the influenced nodes could automatically trace back on finding which node triggers origin of the misbehavior. When the request log entry was damaged at the destination node, the NetPro could trace and find the log request back to the preceding hop node, while another injured log entry has been located. The origin of an observed event was represented as the events chain that comprises the node path, which has generated the fault to present device. The corresponding backward trace has linked the event to the real cause(s). The chain was represented as the event provenance [22]. First, Authors used Ndlog in reasoning expected log and then checking of whether the destination has been influenced or not is done. Due to these experiments, it is proven that NetPro is scalable and practical for use on real MANET routing security [22].

In [23] authors explained the enhanced model for the secured transmission through the initiation of ant colony optimization based clustered based routing protocol (ACO-CBRP). The nodes having the

appropriate trust values enable the calculation of the trust tables of the MANET for detecting the jellyfish attacks [23].Data transmission is done using secured key management [23]. The nodes which are having suitable trust values could enable the assessment of MANET trust tables to detect the jellyfish attacks in the network [23].

In MANET, providing authentication and security to location-based routing is a crucial task. In [24] there is a defense over Sybil attacks and also authentication for anonymous location-based routing in MANET. Each random forwarder node equipped with table of RSS values estimated from the previous message exchanges across a zone to detect the Sybil attack.

Following table 2 and table 3 summarizes the approaches discussed above with features, challenges and highlights major methods and drawbacks.

Author [citation]	Methodology	Features	Challenges
Gimer *et al*. [17]	Multipoint Relay (MPR) nodes	• Improvement in security • Performance ratio is good	• Decreases the chances of construction of multiple disjoint path
Chang *et al*. [18]	cooperative bait detection scheme (CBDS),	• Good packet delivery ratio • Better performance over routing overhead	• Feasibility of the scheme is still in research. • Message integration needs improvement.
Sathiamoorthy *et al.* [19]	Three Fish algorithm	• Reduced Routing overhead	• Lack of data transmission security assurance • Vulnerable to data interruption.
VijayLaxmi *et al*. [20]	JellyFish attack	• Improvement in Scalability measures • Network throughput is achieved more	• Accuracy need to be improved • Needs observation in monitoring process
MarjanKuchaki *et al*. [21]	FbeeAd-Hoc	• Ability to counter the attack.	• Optimization concept is required.. • Selfish node Detection is impossible.
Teng *et al.* [22]	NetPro	• Detection of the direct and indirect attacks automatically. • Can trace the malicious node	• Additional security mechanism needs to be adopted for effective routing.
Satheeshkumar and Sengottaiyan [23]	Collaborative Bait Detection Scheme (CBDS).	• Assures effective route selection • Eliminates the major security issues.	• Additional strategies should be implemented for prevention from Sybil attack • Performance metrics may be improved
Vadhana *et al.* [24]	Location-based routing	• Packet drop attack detection is easy.	• Still suffers from malicious nodes.

Table 2- Summarizing approaches with features and challenges

Sr . No.	Method	Major Drawbacks
1	Proactive detection methods	Required to frequently monitor the nearby mobile nodes to detection malicious nodes. Therefore regardless of malicious nodes existence, the overhead of detection is constantly created, and the resource used for detection is constantly wasted.
2	Reactive detection methods	Initiated the process of malicious nodes detection only when the significant packet drop reported at destination node. So possibility of packet loss introduced moderately by attacker in such methods.
3	Hybrid detection methods	These methods exploited the advantages of both proactive and reactive routing protocols; however the additional care of efficient algorithms design and monitoring is missing.

Table 3- Major methods and drawbacks

In addition to this work the following implementation constraints has been identified by literature survey:

1. The limitations of some current methods is that malicious nodes may still exist in the new chosen route, and this scheme is prone to repeated route discovery processes, which may lead to significant routing overhead.
2. The existing methods under all the categories proposed so far the MANET security failed to estimate the exact cause of performance drop. Without knowing the reasons, the security methods marked the legitimate node also as malicious node. This is most significant challenge of the current MANET security
3. The current security method for MANET does not consider the link quality/congestion parameters while detecting malicious nodes
4. The methods studied in literature failed to achieve the trade-off between the detection rate performance and QoS (Quality of Service) performance as most of the techniques based on dropped PDR or packet losses as key parameter to marked node as malicious.
5. There is absence of security method that conducts the two stage verification to correctly detect the malicious nodes by considering the other causes of packet losses.

III. MOTIVATION AND RESEARCH QUESTIONNAIRE

Sr No	Question	Motivation
1	What is the current status of Malicious Node Detection System for MANET?	(a) stand-alone, (b) cooperative, and (c) hierarchical
2	Which architecture is popular among various Detection Schemes?	Cooperative
3	Why Security is important in MANET?	Security is one of the important aspects in MANET to prevent malicious and evil-intentioned users from disrupting the normal working of the network.
4	What are the other security mechanisms for enhancing security in MANET?	Trust Mechanisms secure data forwarding by isolating nodes with malicious intentions using trust value on the nodes.
5	Whether the existing Detection Scheme based security solutions are sufficient?	Existing methods of intrusion detection have to be modified and new methods have to be defined
6	Does Detection Scheme deployment in MANET has any impact on performance of network?	Yes. Performance metrics needs to be defined. This should be extended for research study.
7	Where the DS should be deployed for maximum performance and detection?	A detection system (**DS**) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered
8	Is it possible to employ some proactive security solutions along with DS in MANET?	Prior detection of attacks and malicious user from the network improves network performance as it reduces the effect that can be caused by that malicious user

9	Which simulation tools are available for traffic and network analysis and best suited for testing the performance of DS in MANET?	It is very important to identify distinct as well as suitable simulation tools for MANET.
10	On the basis of types of information sources- which are the types of IDS?	Host-based IDS, Network-based IDS, Wireless-based IDS, Hybrid

Table 4 –Set of research questions and Motivation

3. 1 Review techniques and strategies applied

This section elaborates the motivating factors for conducting this research on Detection Scheme on MANET also the review strategy used in detail.

3.1.1 Review plan

Stages involved in this literature review on Detection Scheme for MANET includes building a framework of review, downloading research articles from the online libraries, analyzing the survey, understanding the results of the review, recording the results and finally concluding with the research challenges involved

3.1.2 Research questionnaire

The very first step in the literature review involves formation of research questionnaire and finding for relevant papers in different online databases and identifying existing techniques. Table2 gives the set of research questions and corresponding motivation.

3.1.3 Source of information

Different online databases were searched for finding the relevant resources to conducting this survey. These include Springer (www.springer.com), Google Scholar (scholar.google.com), Science Direct (www.sciencedirect.com), IEEE Explore (www.ieeeexplore.ieee.org), ACM Digital library (www.acm .org), WileyInterscience (www.interscience .wiley.com)etc.

3.1.4 Data extraction

The relevant outcome from each of 25 research papers was extracted after an in-depth review. Verification and cross checking of review outcomes were checked in this step.

3.1.5 Study and analysis of references in the article

A brief study of articles in term of a number of citations of an article has also been done in this review. Figure 8 describes process followed for conducting literature survey

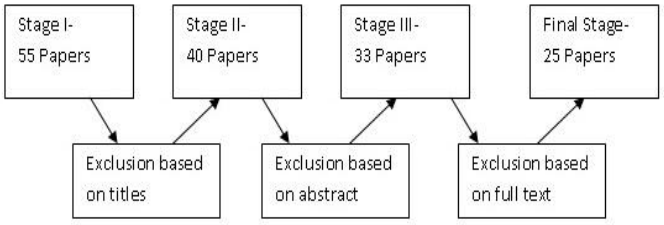

Figure 8 –Conducting literature survey

3.2 Features and Requirements of detection schemes

Following are the features and requirements for ideal detection scheme:-

•Deployment of scheme in MANETs should not introduce new major weakness.
• Over-head should be optimal.
•No modifications/ up-gradations to the existing infrastructure of MANET.
•It should provide real-time automated protection against malicious nodes without any human interaction.
•It should have the mechanism of self-defense and should be able to monitor itself in the case of compromised by the attacker or not.
•It should be interoperable with other detection schemes if required.
•It should have high detection rate and minimal detection time.
•Detection scheme should not only detect the attack but also capable of identifying the source of the attack.
•It should perform equally for both low density and high density network without affecting the performance metrics.
•The mobility of the nodes should be taken into consideration while detection of the malicious node.
•It should have ability to detect multiple attacks with equal efficiency.

3.3 Design consideration for detection scheme

High mobility, resource constraints, absence of any centralized authority for data management, lack of well-defined boundaries, network topology are the main design consideration for a MANET [25].

IV. Brief Overview of Proposed Work

The major aim of this research is to present an idea of the bait detection method for Mobile Ad Hoc Networks (MANETs) with goal of security and routing performance improvement. The proposed method is based on the technique known as CBDS (Cooperative Bait Detection Scheme) which is intended for defending against different types of attacks in MANET. Improved CBDS (ICBDS) method is required to propose with goal improving end to end delay and PDR performances. The results of proposed work against existing CBDS methods will claim that the performance of end to end delay and PDR will be improved for any numbers of attackers in network.

Figure 9 is showing the system architecture with existing and proposed approach which will be adopted for practical work analysis.

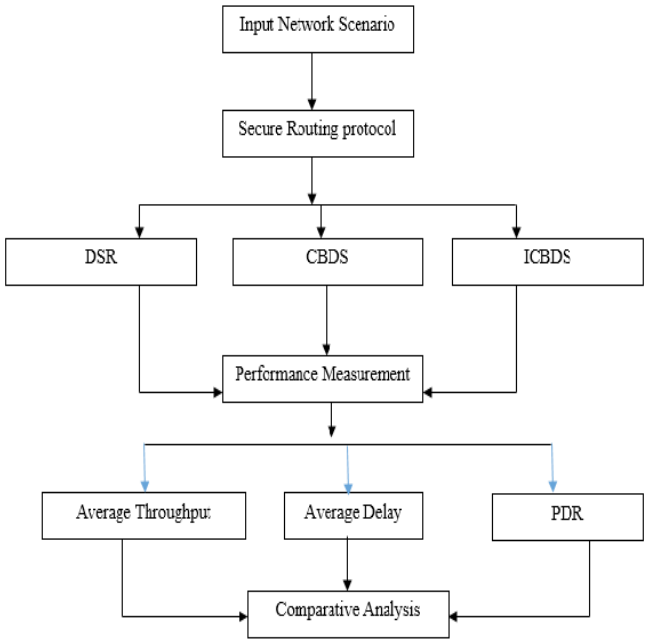

Figure 9- Proposed framework to detect malicious nodes attack in MANET.

V. Conclusion and Future Work

For MANET, security is important research challenge in order to defend against malicious, selfish, and grayhole attacks. In this paper we have categorized attacks in MANET which are responsible for disrupting the routing process. Source routing protocol DSR and the methods like watchdog, TWOACK, AACK, EAACK, CBDS have been discussed with pros and cons. Existing methods fails to estimate exact cause of performance drop, so it is required to design the novel two stage improved cooperative bait detection system for MANETs based on reverse tracking function as well as packet loss analysis. The proposed ICBDS method will outperform the performance of previous DSR and CBDS methods.

To increase the merits of research, it is required to investigate different possibilities of adopting hybrid techniques to further reduce the network overhead. It is also required to achieve optimum solution to detect malicious nodes with better performance metrics. Another future direction is to use efficient cryptography technique which will help to secure the data communication.

REFERENCES

[1] Jian-Ming Chang, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", Published in: IEEE Systems Journal (Volume:9 , Issue: 1), 2014.
[2] Chetan S. Arage, K. V. V. Satyanarayana, "Improved Cooperative Bait Detection Method using Multiple Disjoint Path Technique" Indian Journal of Science and Technology, Vol 9(41), DOI: 10.17485/ijst/2016/v9i41/94793, November 2016.
[3] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.
[4] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008.
[5] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE Int. Conf. Perform., Comput., Commun., 2004, pp. 747–752.
[6] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless Conf., 2003, pp. 75–78.
[7] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.
[8] K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc networks on the mobile value system," in Proc. 2nd Conf. m-Bus., Vienna, Austria, Jun. 2003.
[9] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.
[10] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).
[11] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1983.
[12] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.
[13] D. Johnson, D. A. Maltz, and 3. Broch. The Dynamic Source Routing Protocol for Mobile Ad Hoe Networks (Internet-Draft). Mobile Ad-hoc Network (MANET) Working Group, IETF, October 1999.
[14] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.
[15] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.
[16] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," Wireless Pers.Commun., vol. 29, pp. 367–388, 2004.
[17] GimerCervera, MichelBarbeau, JoaquinGarcia-Alfaro and EvangelosKranakis, " A multipath routing strategy to prevent flooding disruption attacks in link state routing protocols for MANETs", Journal of Network and Computer Applications, vol. 36, no. 2, pp.744-755, March 2013.
[18] J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao and C. F. Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," in IEEE Systems Journal, vol. 9, no. 1, pp. 65-75, March 2015.
[19] J.Sathiamoorthy, B.Ramakrishnan and Usha, " Design of a proficient hybrid protocol for efficient route discovery and secure data transmission in CEAACK MANETs", Journal of Information Security and Applications, vol. 36, Pages 43-58, October 2017.
[20] VijayLaxmi, ChhaganLal, M.S.Gaur and DeepanshuMehta, " JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET", Journal of Information Security and Applications, vol. 22, pp. 99-112, June 2015.
[21] MarjanKuchaki Rafsanjani and HamidehFatemidokht, " FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs", AEU - International Journal of Electronics and Communications, vol. 69, no. 11, pp. 1613-1621, November 2015
[22] Teng Li, Jianfeng Ma and Cong Sun, " NetPro: detecting attacks in MANET routing with provenance and verification", Science China Information Sciences, 2017.
[23] S. Satheeshkumar and N. Sengottaiyan, " Defending against jellyfish attacks using cluster based routing protocol for secured data transmission in MANET", Cluster Computing, pp. 1-12, 2017.
[24] S. Vadhana Kumari and B. Paramasivan, " Defense

against Sybil attacks and authentication for anonymous location-based routing in MANET", Wireless Networks, vol. 23, no. 3, pp. 715–726, 2017.

[25] Sparsh Sharma, AjayKaul "A survey on Intrusion Detection Systems and honeypot based proactive security mechanisms in VANETs and VANET Cloud" Vehicular Communications 12 (2018) 138–164, https://doi.org/10.1016/j.vehcom.2018.04.0052214-2096/