Volume 1, No. 4, Nov-Dec 2010
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

A Survey on DoS Attacks and Countermeasures in Mobile Ad Hoc Networks

M. Gunasekaran*
Department of Computer Applications
Bannari Amman Institute of Technology
Tamilnadu, India
sangraghav@gmail.com

K. Premalatha
Department of CSE
Bannari Amman Institute of Technology
Tamilnadu, India
kpl_barath@yahoo.co.in

B. Gopalakrishnan
Department of Computer Applications
Bannari Amman Institute of Technology
Tamilnadu, India
bgopal1977@gmail.com

Abstract: Security is a critical and significant issue when implementing Mobile Ad Hoc Networks (MANET). Due to the unique nature, such as dynamic topology, limited bandwidth and limited battery power pose both challenges and opportunities in achieving security requirements such as confidentiality, authenticity, integrity, availability and non-repudiation. Various kinds of attacks affect the functionality of different layers in ad hoc networks. There is a kind of harmful attack called Denial-of-Service (DoS) attack that exhibit in multiple forms across different layers of protocol stack. There are numerous mechanism have been designed based on cryptographic primitives and Intrusion Detection Systems (IDS) against DoS attack. This paper provides a survey on DoS attacks and countermeasures in MANET.

Keywords: MANET, Security Attacks and DoS Attack.

I. INTRODUCTION

MANET is a collection of mobile hosts utilize multi-hop radio relaying and are capable of operating without any fixed infrastructure. These nodes have the ability to configure themselves because of the self configuration ability and a node can serve as a router to forward the data to the neighbor's nodes. There is no restriction on the nodes to join or leave the network, therefore the nodes join or leave freely and also these networks have no centralized administrator. This property of the nodes makes the MANET unpredictable from the point of security and routing in particular.

MANET often suffer from security attacks proposed by Wu et al. (2006) compared to wired networks or infrastructure-based wireless networks because of its features like open medium, changing its topology dynamically, lack of central authority, limited energy and resource. These factors have changed the battle field situation for the MANET against the security threats. The wireless and distributed nature of MANET poses a great challenge to system security designers due to the unique nature of the wireless network and is more susceptible to attacks ranging from passive eavesdropping to active interfering. The lack of Certification Authority (CA) or Trusted Third Party (TTP) adds the difficult to deploy security mechanisms and mobile devices tend to have limited power consumption and computation capability which causes it more to DoS attacks.

Security attacks proposed by Rangara et al. (2010) can be categorized on the basis of the source of the attacks i.e. internal or external. External attackers are mainly outside the networks who want to get access to the network and once they get access to the network they start sending bogus packets to disrupt the performance of the whole network. In internal attack, the attacker wants to have normal access to the network as well as participate in the normal activities of the network. The attacker gain access in the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behavior. Internal attack is more severe than external attacks.

The security attacks can also be categorized on the behavior of the attack proposed by Tapaswi et al. (2010) i.e. passive or active. Active attacks can be internal or an external. The active attacks are meant to destroy the performance of network in such case the active attack act as internal node in the network. Being an active part of the network it is easy for the node to exploit and hijack any internal node to introduce bogus packets or DoS. This attack brings the attacker in strong position where attacker can modify, fabricate and replays the massages. Attackers in passive attacks do not disrupt the normal operations of the network. Instead, it listens to the network in order to know and understand how the nodes are communicating with each other, how they are located in the network.

Table I shows the various types of security attacks proposed by Siva Ram Murthy and Manoj (2004) against MANET.

This paper proposes the study of security threats which induce DoS attacks on various layers of the protocol suite and described in detail about the issues. And also discusses the existing security mechanism proposed by various authors against DoS attacks using first line of defense such as cryptographic primitives and as a second line of defense such as IDS.

Table I. Security Attacks on protocol stack

Security Attacks	*Targeted Layer*
Repudiation	Application layer
Session hijacking SYN flooding	Transport layer
Wormhole Blackhole Byzantine Flooding Location Disclosure Information Disclosure Routing attacks	Network layer
Jamming	Data link layer
DoS, Impersonation	Multi-layer attacks

This paper is organized as follows. Section II presents an overview of DoS attacks on various layers in protocol stack. Section III provides an overview of countermeasures against DoS attacks. Section IV gives the statistical analysis of countermeasures. Section V presents conclusion and discuss future directions.

II. DOS ATTACKS IN MANETS

Siva Ram Murthy and Manoj (2004) & Wu et al. (2006) proposed DoS attacks that could be initiated from various layers in MANET. Therefore, DoS attacks may impact the network connectivity seriously and may further undermine the network functionalities, such as data and control packet delivery. In addition to that it consumes the system resources, such as battery power and bandwidth and also isolates legitimate users from accessing information or services in the network. Due to the malicious behavior of the node DoS attacks may be initiates almost in all layers.

In transport layer a malicious node,

[a] A malicious node send large amount of SYN (Synchronization) packet to the target node. These SYN packets can be from spoofed source addresses of unreachable nodes. If the attacker is spoofing source addresses from nodes that are unreachable, the target node will attempt to complete the session by sending back SYN ACK (Acknowledgement) packets which will never be acknowledged or reset.

In network layer a malicious node,

[a] Floods large number of packets to the victim to prevent victim or the whole network from establishing or continuing communications and consume victim's bandwidth and battery power.
[b] Participates in a route but simply drops some of the data packets.
[c] Transmits falsified route updates.
[d] Copies a forwarded packet and later sends out the copies repeatedly and continually to the victim's buffers to drain the power supply or to consume bandwidth.
[e] Could deny the availability of the existing route or intentionally forward data packets to the wrong destination.

In Physical and Media Access Control (MAC) layer a malicious node,

[a] can effectively cut off wireless connectivity among nodes by transmitting continuous radio signals such that other authorized users are denied from accessing a particular frequency channel (keeping that channel busy)
[b] Transmit jamming radio signal to intentionally collide with legitimate signals originated by target node

Table II shows the example of a classification of DoS attacks on different layers of the protocol suite.

Table II. DoS Attack on different layers

DoS Attacks	*Targeted Layer*
SYN Flooding	Transport layer
Flooding Resource Consumption Packet Drop Replay Stale Updates Falsified Route Updates	Network layer
Jamming Collision	Data link layer
Jamming Tampering	Physical layer

The following sub-sections describe different types of security threats which induce DoS attacks in MANETs.

A. Jamming Attack

Interference can happen either accidentally or intentionally with radio waves of MANET. A radio signal can be jammed or interfered, which causes the message to be corrupted or lost. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overwhelm the targeted signals and disrupt communications. The most common types of this form of signal jamming are random noise and pulses.

B. Collision Attack

In wireless networks, the channel is reserved for transmission through RTS (Request To Send) / CTS Clear To Send) packets. In spite of the channel reservation, an adversary node can induce a collision in the wireless channel by transmitting when another node in the range is already in transmission. The purpose of this attack is either to prevent access to a certain node or to exhaust the transmitting nodes resources by continuous retransmissions.

C. Flooding Attack

Malicious node deliberately floods the whole network with meaningless Route Request (RREQ) and Route Reply (RREP) packets. The purpose of doing so is to paralyze the network by destroying its routing logic and to exhaust the network bandwidth. Such attacks are possible only because RREQ and RREP packets are not authenticated. Any body can forge such messages. The only solution for these attacks is to authenticate route control messages.

D. Packet Dropping Attack

It is possible for malicious nodes to modify the packet content, if proper integrity checks are not maintained. Also it is possible to change the header information including source address, destination address and Time-To-Live (TTL) value. The malicious intermediate nodes can also simply drops data or route packets. Some variations of packet dropping based on frequency and selectiveness are selective dropping, constant dropping, periodic dropping and random dropping.

E. Packet Misdirection

Misdirection attack occurs when the adversary node forwards the data packet to the wrong destination. In another kind of misdirection attack is the adversary node deny the availability of an existing route to the destination by sending false route error messages thus preventing service to the destination in the absence of alternate routes.

F. Rushing Attack

In rushing attack, a malicious node wants a route to be established through it. For this purpose, a malicious node waits for RREQ of sources either selectively or collectively. Whenever the RREQ arrives, the malicious node rushes the request to the next intermediate node, in a hope to get a route through it. The probability of getting a route through malicious node is higher, because of the property of all nodes to select the first RREQ and forward it, and discarding the duplicate RREQ. If the RREQ forwarded by the attacker are the first to reach each neighbor of the target, then any route discovered by this route discovery will include a hop through the attacker. Note that even if secure routing is used, this attack is possible. The malicious node can do harm to other nodes or network after a route is established through it. The rushing attack acts as an effective DoS attack against all currently proposed on demand ad hoc network routing protocols, including secure routing protocols.

G. Replay Attacks

In a MANET, topology frequently changes due to the high node mobility. This means that current network topology might not exist in the future. In replay attack, a node records another nodes valid control messages and resends them later. This causes other nodes to record their routing table with stale updates. Replay attack can be misused to impersonate a specific node or simply to disturb the routing operation in a MANET.

III. COUNTERMEASURES AGAINST DOS ATTACKS IN MANETS

A variety of security mechanisms have been proposed by various authors against DoS attacks. The conventional approaches such as symmetric cryptography, asymmetric cryptography, key management algorithm and identity based cryptography have been used as a first line of defense. Second line of defense such as, Intrusion Detection Systems (IDS) has been used to detect misuse and anomalous in MANET.

A. Preventive Mechanism

The conventional authentication and encryption schemes are based on cryptography, which includes asymmetric and symmetric cryptography. Symmetric cryptographic primitives such as hash functions (message digests), shared key, random nonce and message authentication code and asymmetric cryptography primitives such as digital signatures, certificate authority and identity-based cryptography.

This section provides the various solutions provided by the different authors with respect to jamming, malicious behaviours against DoS attacks in MANET.

[a] Solutions against Jamming

Hamieh and Ben-Othman (2009) proposed a model based upon the measure of statistical correlation to detect specific type of jamming, in which the jammer transmits only when valid radio activity is signaled from its radio hardware. At other times, the attacking device enters sleep states while its radio passively listens. Using this strategy, the attacker also saves energy and decrease the probability of detection by jamming the packet.

Pelechrinis et al. (2010) considered a malicious node that continually transmits a radio signal in order to block any legitimate access to the medium and/or interfere with reception. However this type jamming techniques mainly exploit PHY and MAC layer vulnerabilities. Jammers have responded by employing more intelligent ways to accomplish jamming task in order to evade detection. They exploit vulnerabilities at the higher layers of the network stack. This paper addresses mainly jamming attacks with respect to PHY and MAC layer and discussed about anti-jamming strategies to detect and prevent jammers.

Popper et al. (2010) proposed three instances of uncoordinated spread spectrum techniques that enable anti-jamming broadcast communication without shared secrets and to handle unlimited amount of malicious receivers. The author uses three instances, the Uncoordinated Frequency Hopping (UHF), Uncoordinated Direct Sequence Spread Spectrum (UDSSS) and hybrid UFH-UDSSS. UFH resembles Frequency Hopping but randomizes the selection of the frequency channels while UDSSS randomizes the selection of the spreading codes. And the authors also discussed different applications of USS techniques including emergency alert broadcasts and navigation.

[b] Solutions against malicious behaviors

Sanzgiri et al. (2005) considered variety of attacks, such as modification routing messages or impersonation of other nodes, can allow attackers to influence a victim's selection of routes or enable DoS attacks. They have developed Authenticated Routing for Ad Hoc Networks (ARAN), used public-key cryptographic mechanisms to defeat all identified attacks and also showed ARAN can secure routing in environments where nodes are authorized to participate but un-trusted to cooperate, as well as environments where participants do not need to be authorized to participate. ARAN provides authentication and non-repudiation services using cryptographic certificates that guarantees end-to-end authentication. The computational overhead is larger, which result in a higher overall routing load, and higher latency in route discovery because of the cryptographic computation.

Yi et al. (2005) developed Flooding Attack Prevention (FAP) mechanism against flooding attack in MANETs. The FAP is composed of neighbor suppression and path cutoff. In this approach, when the intruder broadcasts exceeding packets of route request, the immediate neighbors of the intruder observe a high rate of route request and then they lower the corresponding priority according to the rate of incoming queries. Mainly the not serviced low priority queries are eventually discarded. When the intruder sends many attacking data packets to the victim node, the node may cut off the path and does not set up a path with the intruder any more. The FAP prevents flooding attack in MANETs with little overhead.

Tan and Seah (2005) used statistical filtering to oppose DDoS attacks in MANETs. The authors discussed the effectiveness of DDoS attacks on automated statistical filtering in wired networks and proposed a framework to adopt such statistical filtering mechanisms in MANETs that make use of a cluster-based approach. And also the authors simulated some DDoS attacks in MANETs without any filtering mechanisms to explore and understand the effects of such attacks on the performance of the network.

Wei et al. (2007) proposed a solution using against packet dropping. The solution consists of two algorithms: the key management algorithm based on gossip protocol by assume all nodes own initial public key certificates and the detection algorithm based on aggregate signatures. The distributed Certificate Authority (dCA) has a public/private key pair, and the private key is shared among the dCA servers. In this mechanism, (i) only dCA exists, and no mother Certificate Authority (mCA) exists, (ii) all signatures are certificate-based signatures, (iii) dCA servers perform a proactive certificate-signing key share update.

Wu and Yau (2007) proposed a DoS mitigation technique that uses digital signatures to verify legitimate packets, and drop packets that do not pass the verification. Since selfish nodes may not perform the verification in order to avoid paying the overhead. A bad packet that escapes verification along the whole network path will bring a penalty to all its forwarders. A network game can be formulated in which, nodes along a network path, in optimizing their own benefits, are encouraged to act collectively to filter out bad packets.

Xiaopeng and Wei (2007) used firstly aggregate signature algorithm to trace packet dropping nodes. Secondly they proposed three related algorithms: the creating proof algorithm, the checkup algorithm and the diagnosis algorithm. The first one was for creating proof, and the second one was for checking up source route nodes, and the last one was for locating the malicious nodes. The protocol detects malicious nodes and the false positive rate, routing packet overhead is low and also the packet delivery rate has been improved.

Guo and Perreau (2007) presented a behavior-based traceback mechanism to identify flooding attack in MANETs. In addition, the authors proposed an attack isolation scheme to alleviate the attack impact on the network. This approach traces multi-sources and distributed flooding attacks in MANET. By observing different behaviours of malicious and innocent nodes, the traceback mechanism can identify malicious nodes or areas accurately no matter whether they use address spoofing or not. And also the authors proposed an attack isolation scheme, working parallel with the tracing procedure, to alleviate attack impact on the network: the attack traffic is limited in a certain area and network throughput loss is retrieved at most.

Balakrishnan et al. (2007) proposed a Trust Integrated Cooperation Architecture which consists of an obligation-based cooperation model known as fellowship to defend against both was flooding and packet dropping attacks. Further, the security decisions of fellowship may be enhanced through a Secure MANET Routing with Trust Intrigue (SMRTI) that evaluates the trustworthiness for other nodes in order to enhance the security decisions of fellowship model. SMRTI is free from honest-elicitation, free-riding, bias of a recommender, and additional overhead.

Aad et al. (2008) used quantitative methodology against JellyFish (JF) and Blackhole attacks. The authors considered the performance metrics as system fairness, number of hops for received packets, total system throughput and probability of interception to evaluate the impact of JF on individual flows, as well as on the whole system performance. And also showed that, how such attacks actually increase the capacity of ad hoc networks as they will starve all multi-hop flows and provide all resources to one-hop flows that cannot be intercepted by JellyFish or Black Holes.

Nakayama et al. (2009) proposed anomaly-detection scheme based on a dynamic learning process that allows the training data to be updated at particular time intervals. The author used the current time interval and first time interval. By using the data collected in first time, initially, the first principal element is calculated, and then the calculated first principal element is used in the following time interval that is current interval time for anomaly detection. If the state in current interval time is judged as normal, then the corresponding data set will be used as the training data set. Otherwise, it will be treated as the data including attack, and it will consequently be discarded. This way, the approach keeps on learning the normal states of the network. The proposed system also demonstrates an effective performance in terms of high data rate and low false positive rate against attacks.

Khabbazian et al. (2009) proposed a proactive countermeasure based on time analysis. Timing analysis techniques are based on the fact that a packet can travel at most at the speed of light. Therefore, a node can estimate its distance to a sender by multiplying Packet Travel Time (PTT) by the light speed. Each node can validate vicinity of all its neighbors in two rounds of communication. In the first round, each node sends a signed Hello message containing its ID and a nonce, and records the time at which the message is fully sent. It follows that after the first round, each node has a list of all its potential neighbors. In the second round, each node signs and sends a follow-up packet. The follow-up packet includes the time at which the node's Hello message was sent (in the first round), the list of all the ID's in the received Hello messages together with their corresponding nonces and the times at which they were received. Nonces are used to prevent malicious nodes to masquerade a legitimate node. Note that neither Hello messages nor follow-up packets are timestamped with their transmission time. Therefore, the nodes do not require computing a signature while having to timestamp the packet with its transmission time.

Yu et al. (2009) proposed a routing algorithm which detects an internal attacks by using both message and route redundancy during route discovery. A node builds up the trustworthiness on its neighboring nodes on its observations on the behaviors of the neighbor nodes. The node also makes a routing decision based on its trust of its neighboring nodes and the performance provided by them. The computational burden at each node is still a major issue in deployment and it needs both analytical investigations and engineering considerations. Considering the mobility this protocol is expected to increase the prediction accuracy and thus reduce the link breakage rate during deployment.

Lu et al. (2009) implemented an Ad Hoc On-Demand Distance Vector (AODV) routing protocol suffering black hole attack, namely Bad Ad Hoc On-Demand Distance Vector (BAODV) routing protocol and showed that the network performance of MANET using BAODV is very worse than using AODV. The authors developed a Secure Ad Hoc On-Demand Distance Vector (SAODV) protocol; it directly verifies the destination node by using the exchange of random numbers. They have also showed how effectively SAODV prevent black hole attack, maintain a high routing efficiency and improve the network performance.

Yil et al. (2009) analyzed the flooding attack on the entire network performance under the circumstances of different flooding frequency and different number of attack nodes. To reduce congestion in a network, the existing protocol (DSR, AODV, DSDV and others) adopts various constraints. But the attacker node violates the constraints to exhaust the network resources. The authors showed that, with the increase of flooding frequency and the number of attack nodes, network performance drops. When the frequency of flooding attacks in less than a certain value, network performance decreases in inverse proportion to the increasing frequency of attacks. But when the frequency of flooding attacks is greater than the value, the performance decrease gets smooth. In addition, with the increasing frequency of flooding attacks, the packet delay firstly increases and then declines to a value of stability in the end.

Xing and Wang (2010) proposed a semi-Markov process model to characterize the evolution of node behaviors and investigated the problem of node isolation where the effects of DoS attacks are considered. In this (i) semi-Markov process (SMP) is used to characterize the evolution of node behaviors, and the stochastic property of the model is analyzed to disclose the effects of node behaviors (ii) node isolation problem is revisited by examining the cooperative degree, and the probabilistic k-connectivity of individual nodes is obtained by using the stochastic property of node behaviors and (iii) survivability of wireless ad hoc networks is analyzed probabilistically, and its theoretical bounds are derived in closed forms, which is used to quantify the impacts of different behaviors.

Kim et al. (2010) proposed a period-based defense mechanism against data flooding attacks. The current defense systems focus on RREQ flooding attacks rather than the data flooding attack. They easily reduce the throughput of burst traffic by comparing with the simple threshold. The proposed scheme uses a blacklist, considers the data type, and processes packets according to the priority so as to defend against data flooding attacks; since the attacker forwards many data packets at a high rate for the whole session. The proposed scheme is useful to networks where burst traffics are transferred because many users tend to download and share multimedia data.

B. Reactive Mechanism

An Intrusion Detection System serves as a second line of defense, after first line of defense by prevention techniques, which detects malicious activities in a network and also has the ability to detect or provide a view of malicious activities. This mechanism collects data from legitimate user behavior over a period of time, and then statistical tests are applied to determine anomalous behavior with a high level of confidence. The two major analytical techniques are:

a. Misuse detection: It uses signature of known attacks, to identify those attacks
b. Anomaly detection: It uses established normal profiles only to identify any unreasonable deviation from them.

This section discusses the solutions provided by various authors with respect to multiple layers that cross-layer design against DoS attacks in MANET.

[a] Cross Layer Design against DoS

Thamilarasu et al. (2005) proposed a Cross layer based Intrusion Detection System (CIDS) to identify the malicious node(s) and provided a host based IDS that resides in every host and monitors its local neighborhood for abnormalities in the network activities. The authors used different approaches to detect collision, packet drop and misdirection in which every layer of the protocol stack interacts with the IDS module. When collision occurs, the link layer marks a set of nodes as suspicious and these nodes are fed to the IDS detection module. The packet drop is implemented at the network layer, where the detected nodes are fed into the IDS. CIDS gets the information fed from the collision detection at the link layer and packet drop and/or misdirection at the network layer. The IDS, based on this information confirms the suspected node to be malicious with a certain degree of confidence and by triggering multiple detections increase the accuracy of IDS.

Chen et al. (2006) proposed ThroughpUt-Feedback routing (TUF) architecture, which is resilient to a wide range of attacks, including protocol-compliant attacks. TUF is composed of two modules: Throughput Monitoring (TM) and Route Rebuilding (RR). TM is responsible for detecting any abnormalities that might occur on a route. If any abnormalities are detected, TM invokes RR, which employs the Least-Alike Re-Routing (LARR) algorithm to build a new route. The authors showed that how effectively TUF mitigate protocol-compliant attacks and also showed TUF is capable of circumventing a variety of insider attacks such as blackhole, grayhole, rushing, and wormhole attacks.

Hejmo et al. (2006) proposed cross-layer architecture for QoS signaling in MANETs, which provides resistance to a class of DoS attacks. The proposed DoS-Resistant QoS (DRQoS) signaling scheme employs distributed rate control to manage the bandwidth resources of the network, but does not rely on the maintenance of per-flow state. In this scheme, each mobile node maintains a state table of bandwidth reservations, which grows as a function of the number of neighbor nodes rather than the number of traffic flows traversing the node. The DRQoS protocol provides QoS signaling on top of an arbitrary MANET routing protocol and employs mechanisms at the MAC layer for QoS provisioning and resistance to attacks in conjunction with the signaling protocol. The key MAC layer elements of the scheme consist of estimating the available wireless bandwidth, traffic policing, and rate monitoring, all of which are performed in a distributed manner in the network. But this solution prone to state table exhaustion.

Bose and Kannan (2008) proposed a cross-layer based framework against DoS attacks that is collisions at MAC layer, packet drop and misdirection in the network layer. These multi-layer solutions exploit the information available across different layers of the protocol stack by triggering two levels of detection that enhances the accuracy. Level-1

detection triggers selecting a monitor for analyzing the trace files to detect the intruder. Level-II detection collects information about the intruder from multiple layers. To confirm the suspicious behavior of the malicious nodes, the information obtained from various layers of protocol stack is combined to determine the commonality of nodes among them. This approach reduces the false positives.

Liu et al. (2009) proposed a framework of combining intrusion detection and continuous authentication in MANET. In this framework, multimodal biometrics is used for continuous authentication, and intrusion detection is modeled as sensors to detect system security state. The whole system is formulated as a partially observed Markov decision process considering both system security requirements and resource constraints and used dynamic programming-based hidden Markov model scheduling algorithms to derive the optimal schemes for both intrusion detection and continuous authentication.

Shrestha et al. (2010) presented a secure IDS system that detects attacks on Authenticated On-Demand Distance Vector (AODV) routing protocol by using anomaly detection technique. The intrusion detection system is built in a distributive manner that can trace the flaws or attacks on the AODV routing protocol with one way key chain authentication which makes the system more robust against attacks because the nodes first have to authenticate themselves to other neighboring nodes before starting communication. Intrusion detection involves capturing audit data and reasoning about the evidence in the data to determine if the system is under attack or not. Depending on the scope of protection or deployment and according to audit data used, IDS can be classified as network-based or host-based. This system detects most of the attacks with low overhead.

Shrestha et al. (2010) proposed cross layer intrusion detection architecture to discover the malicious nodes and different types of DoS attacks by exploiting the information available across different layers of protocol stack in order to improve the accuracy of detection. The authors used cooperative anomaly intrusion detection with data mining technique to enhance the proposed architecture and implemented fixed width clustering algorithm for efficient detection of the anomalies in the MANET traffic. The proposed cross-layer based intrusion detection architecture detects DoS attacks and sinkhole attack at different layers of the protocol stack and also able to detect various types of UDP flooding attack.

El-Khati et al. (2010) proposed a hybrid model which combines the filter and wrapper models for selecting relevant features. This approach efficiently selects the optimal set of features in order to detect 802.11-specific intrusions. The feature selection uses the information gain ratio measure as a means to compute the relevance of each feature and the k-means classifier to select the optimal set of MAC layer features that can improve the accuracy of intrusion detection systems while reducing the learning time of their learning algorithm.

IV. STATISTICAL ANALYSIS

This section summarizes the various security mechanisms provided against the security attacks at different layers that induce DoS attacks. Most of the security mechanisms has a different set of operational requirements and provides protection against mostly one or two attacks in particular by utilizing particular approaches. Some security solutions provide cross-layer based mechanism but those mechanisms also concentrates on one or two malicious activities but not in multi-layers.

From the analysis most of the solutions provided by various authors suffered by high computational overhead because of costly algorithms which intern increases node complexity that degrades the performance of MANET. Energy management is another critical issue because of its unique nature, but no proper consideration and direction about that issue. Most of the solutions focus on network layer that too few attacks in particular, few solutions considered Physical and MAC layers threats but not fully, and no considerations SYN flooding attack on transport layer.

Table III summarizes the results of the comparison and forms a basis of discussion in this section. The table contains various categories of threats in different layers that induce DoS attacks in MANET. This table contains about the various types of security attacks, targeted layer, solutions proposed by various authors, the algorithms and techniques used by authors and the disadvantages of the proposed solutions.

V. SUMMARY AND FUTURE DIRECTIONS

Security is an essential and significant service for wired, infrastructure-based and infrastructureless networks. Because of the unique nature, the success of MANET strongly depends on its security in communication. This paper discussed various types of security threats that induce DoS attacks at various layers of the protocol suite in MANET and their consequences in particular. For countermeasures against DoS attacks, this paper also discussed mainly about jamming, collision at MAC layer, malicious behaviors at network layer and multi-layer attacks.

All the existing solutions are mainly based on first line of defense the cryptographic primitives such as hash functions (message digests), shared key, random nonce, message authentication code, digital signatures, certificate authority, identity-based cryptography and some solutions based as a second line of defense that is IDS.

Our analysis showed that although many solutions have been proposed against DoS attacks that are typically based on the specific layer or multi-layer that too mainly one or two security considerations in each layer. But still there are various security threats in different layers that induce DoS attacks in MANET which are remain undiscovered or not considered. And also these solutions are too expensive, giving high computation overhead and no expected level of confidence among nodes.

However, prevention or detection of DoS attacks is still an open issue. In MANET, DoS attacks are quite common because of its unique nature as mentioned earlier. Firstly at the PHY and MAC layer, secondly at the network layer and thirdly at the transport layer.

One interesting research issue is to build trust-based system using witness anonymity and accountability so that the nodes confidence level could be increased. The anonymity property identify the node who provide feedback in the form of their trust ratings for another node and the

accountability property identify malicious nodes who attempt to misuse the anonymity property to manipulate the trust value computed for a node. In addition to the trust model:

Spread spectrum technology such as FHSS and DSSS can be used against jamming, collision and interception of radio signal in the PHY and MAC layer.

End-to-end authentication and greater TTL value (TTL value > hop count) can be used to defend against malicious attacks in the network layer and transport layer.

Table III. Defense against DoS attacks at specific layer, requirements and drawbacks

Attack Types	*Targeted Layer*	*Proposed Solution*	*Requirement*	*Drawbacks*
Modify or drop packet	N/w layer	ARAN [19]	Trusted certification authority	Higher routing load and latency
Flooding	N/w layer	FAP [31]	Neighbor suppression and path cutoff	No implementation details
Collision, packet drop and misdirection	MAC & N/w layer	CIDS [25]	RTS/CTS and watch-dog monitoring	Higher computational overhead
Routing Disruption, blackhole, rushing and grayhole	N/w layer & Transport layer	TUF [5]	Least-alike re-routing (LARR) algorithm	Experimented in identical network condition
Flooding, replay and resource consumption	MAC and N/w layer	DRQoS [10]	Rate adjustment /monitoring and traffic policing	Prone to state table exhaustion attack
Flooding and packet dropping, Resource consumption	N/w layer	TICA [2]	Fellowship and SMRTI	No implementation
Flooding, Resource consumption	N/w layer	TFA [8]	Quantitative node differentiation principle, node granularity and area granularity	Nodes need more packets and time to identify attackers
Packet dropping	N/w layer	NGHADS [29]	Creating proof algorithm, checkup algorithm and diagnosis algorithm	High computational and space complexity
Packet dropping	N/w layer	RGHA [26]	Gossip algorithm and aggregate signature	High computational overhead
Flooding, replay and resource consumption	N/w layer	DoS Mitigation Technique [27]	Digital signature & game theory	Experimented in identical network condition
Packet drop, reorder, delay	N/w layer	Analytical Model [1]	Analytical modeling and scalability	High computational overhead
Collision, Packet drop and misdirection	MCA and N/w layer	Cross-layer based IDS [4]	Intrusion detection and message passing	No solution about jamming
Packet dropping and misdirection	N/w layer	SRAC [33]	PKI, RSA, Secret Key and CA	Higher computational overhead
Flooding, packet dropping ,misdirection, replay and routing disruption	MAC & N/w layer	Combine [13] intrusion and continuous authentication	Multimodal biometrics, intrusion detection and Markov model	High complexity
Routing disruption or misdirection	N/w layer	Timing based countermeasure [11]	Timing analysis, CTS and RTS	Grid topology gives problem when the malicious nodes are located in main diagonal of the grid
Flooding, packet dropping, misdirection and resource consumption	N/w layer	Anomaly detection scheme [15]	Projection distance, path abnormality, forgetting curve and dynamic learning	Processing overhead is high
Jamming	MAC layer	Detection of jamming attack using error distribution [9]	Correlation, CTS, RTS, DCF and CSMA/CA	Only very few nodes used for simulation
Packet drop, reorder, delay	N/w layer	Semi-Markov process model [30]	Disjoint outgoing paths, semi-markov process, node isolation	Impact of node behaviours on network performance is still problem
Jamming and collusion	MAC and N/w layer	Novel hybrid model [6]	IDS, k-means, information gain ratio, neural networks	Higher computational overhead
Jamming and collusion	MAC and N/w layer	Uncoordinated spread spectrum [17]	DSSS, FHSS	No information about tampering

Flooding and resource consumption	N/w layer	Cross layer intrusion detection [20]	Apriori algorithm, clustering and association algorithm	Node complexity is high

VI. REFERENCES

[1] Aad I, Hubaux J-P and Knightly E. W, "Impact of Denial of Service Attacks on Ad Hoc Networks", IEEE/ACM Transactions on Networking, vol. 16, no. 4, pp. 791-802, 2008.

[2] Balakrishnan V, Varadharajan V, Tupakula U and Lucs P, "Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks", Proceedings of fourth International Conference on Wireless Communication Systems, pp. 592-596, 2007.

[3] Biswas K and Liaqat Ali M "Security threats in Mobile Ad Hoc Network", Master Thesis, Blekinge Institute of Technology, 2007.

[4] Bose S and Kannan A, "Detecting Denial of Service Attacks using Cross Layer based Intrusion Detection System in Wireless Ad Hoc Networks", Proceedings of IEEE-International Conference on Signal processing, Communications and Networking, pp. 183-188, 2008.

[5] Chen R, Snow M, Park J, Refaei M T and Eltoweissy M, "Defense against Routing Disruption Attacks in Mobile Ad Hoc Networks", Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies, pp. 1252-1261, 2006.

[6] El-Khatib K, "Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems", IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 8, 2010.

[7] Gao Xiaopeng Chen Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", Proceedings of International Conference on Network and Parallel Computing, pp. 209-213, 2007.

[8] Guo Y and Perreau S, "Trace Flooding Attack in Mobile Ad Hoc Networks", Proceedings of third International Conference on Intelligent Sensors, Sensor Networks and Information, pp. 329-334, 2007.

[9] Hamieh A and Ben-Othman J, "Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution", in Proceedings of IEEE International Conferences on Communications, pp. 1-6, 2009.

[10] Hejmo M, Mark B. L, Zouridaki C and Thomas R. K, "Design and Analysis of a Denial-of-Service-Resistant Quality-of-Service Signaling Protocol for MANETs", IEEE Transactions on Vehicular Technology, vol. 55, no. 3, pp. 743-751, 2006.

[11] Khabbazian M, Mercier H and Bhargava V. K, "Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks", IEEE Transaction on Wireless Communications, vol. 8, no. 2, pp. 736-745, 2009.

[12] Kim H, Bhargav Chitti R and Song J, "Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks", IEEE Transactions on Consumer Electronics, vol. 56, no. 2, pp. 579-582, 2010.

[13] Liu J, Yu F. R, Lung C-H and Tang H, "Optimal Combined Intrusion Detection and Biometric-Based Continuous Authentication in High Security Mobile Ad Hoc Networks", IEEE Transaction on Wireless Communications, vol. 8, no. 2, pp. 806-815, 2009.

[14] Lu S, Li L, Lam K and Jia L, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", Proceedings of 2009 International Conference on Computational Intelligence and Security, pp. 421-425, 2009.

[15] Nakayama H, Kurosawa S, Jamalipour A, Nemoto Y and Kato N, "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks", IEEE Transaction on Vehicular Technology, vol. 58, no. 5, pp. 2471-2481, 2009.

[16] Pelechrinis K, lliotofou M and Krishnamurthy S. V, "Denial of Service Attacks in Wireless Networks: The Case of Jammers", IEEE Communications Surveys & Tutorials, IEEE Communication Society, pp. 1-13, 2010.

[17] Popper C, Strasser M and Capkun S, "Anti-Jamming Broadcast Communication using Uncoordinated Spread Spectrum Techniques", IEEE Journal on Selected Areas in Communications, vol. 28, no. 5, 2010.

[18] Rangara R. R, Jaipuria R. S, Yenugwar G. N. and Jawandhiya P.M, "Intelligent Secure Routing Model for MANET", Proceedings of 3rd IEEE International Conference on Computer Science and Information Technology, vol. 3, pp. 452-456, 2010.

[19] Sanzgiri K, LaFlamme D, Dahill B, Levine B.N, Shields C and Belding-Royer E.M, "Authenticated Routing for Ad hoc Networks", IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 598-610, 2005.

[20] Shrestha R, Sung J-Y, Lee S-D, Sik-Yun P, Choi D-Y and Han S-J, "A Secure Intrusion Detection System with Authentication in Mobile Ad hoc Network", Proceedings of Pacific-Asia Conference on Circuits, Communications and Systems, pp. 759-762, 2009.

[21] Shrestha R, Han K-H, Choi D-Y and Han S-J, "A Novel Cross Layer Intrusion Detection System in MANET", Proceedings of 24th International Conference on Advanced Information Networking and Applications, pp. 647654, 2010.

[22] Siva Ram Murthy C and Manoj B. S, "Ad Hoc Wireless Networks: Architecture and Protocols, Pearson Eduction, 2004.

[23] Tan H, Seah W.K.G, "Framework for Statistical Filtering Against DDoS Attacks in MANETs", Proceedings of Second International Conference on Embedded Sfotware and Systems, p. 8, 2005.

[24] Tapaswi, Kushwah S, and Singh V, "Securing Nodes in MANETs using Node Based Key Management Scheme", Proceedings of International Conferences on Advances in Computer Engineering, pp. 228-231, 2010.

[25] Thamilarasu G, Balasubramanian A, Mishra S and Sridhar R, "A Cross-layer based Intrusion Detection Approach for Wireless Ad hoc Networks", IEEE International Conference on Mobile Ad Hoc and Sensor Systems, p. 7, 2005.

[26] Wei C, Xiang L, Yuebin B and Xiaopeng G, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of Second International

Conference on Communication and Networking, pp. 366-370, 2007.

[27] Wu X and Yau D.K.Y, "Mitigating Denial-of-Service Attacks in MANET by Incentive-based Packet Filtering: A Game-theoretic Approach", Proceedings of third International Conference on Security and Privacy in Communications Networks, pp. 310-319, 2007.

[28] Wu B, Chen J, Wu J, and Cardei M, "Wireless Network Security", Springer-Verlag, 1st Edition, 2006.

[29] Xiaopeng G and Wei C, " A Novel Gray Hole Attack Detection Scheme for Mobile Ad Hoc Networks", Proceedings of International Conference on Network and Parallel Computing, pp. 209-214, 2007.

[30] Xing F and Wang W, "On the Survivability of Wireless Ad Hoc Networks with Node Misbehaviors and Failures", IEEE Transactions on Dependable and Secure Computing, vol. 7, no. 3, 2010.

[31] Yi1 P, Wu Y and Ma J, "Experimental Evaluation of flooding attacks in mobile ad hoc networks", Proceedings of IEEE International Conference on Communications, pp. 1-4, 2009.

[32] Yi P, Dai Z, Zhong Y and Zhang S, "Resisting Flooding Attacks in Ad Hoc Networks", Proceedings of the International Conference on Information Technology: Coding and Computing, pp. 657-662, 2005.

[33] Yu M, Zhou M and Su W, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 449-460, 2009.

