SURVEY OF MANET MISBEHAVIOUR DETECTION APPROACHES

Punya Peethambaran and Dr. Jayasudha J. S.

[1]Department of Computer Science and Engineering, SCT College of Engineering, Trivandrum, Kerala

[2] Head of the Department, Department of Computer Science and Engineering,SCT College of Engineering, Trivandrum, Kerala

ABSTRACT

Mobile ad hoc networks (MANETs) turn out to be very useful in the current application areas for networks that require ad hoc connectivity as well as mobility. While the MANET routing protocols were designed it was assumed that there is no chance to have a malicious node in the network that does not co operate with each other to transmit data. Because of this fact, the network layer of MANETs is vulnerable to attacks of several kinds. Here in this paper, different kinds of attacks on MANETs are discussed first and then some protection mechanisms against those attacks are discussed. Comparisons of these mechanisms are also included.

KEYWORDS

Mobile ad hoc networks, Attacks, Network Security, Intrusion Detection, Network layer security.

1. INTRODUCTION

A mobile ad hoc network is a group of mobile nodes which do not need an access point or any infrastructure for proper working [1], [2], [3]. Unlike normal network architectures, here in MANETs all nodes work as both sender and receiver. MANETs are widely used in emergency applications mainly due to the two characteristics of self configuration and easy deployment of mobile nodes. Nowadays it is even used in industrial applications extensively. In such a scenario, it is crucial to solve the security issues in them.

In ordinary wireless networks, the communication is limited to the nodes within the range of communication, i.e. the range of the transmitters. In contrary, in MANETs intermediate nodes help in transmission. MANET networks can be classified as of two types, single hop and multi hop. Nodes in a single hop network which are in the transmission range will communicate with each other directly. What happens when the nodes that require communicating are not within the transmission range? It is then that the multihop networks are used. Here, the intermediate nodes will help in transmission, if the communicating nodes are not within the range of communication. The network infrastructure of MANETs is decentralized and is not fixed, which means all the nodes are free to move.

In some of the emergency circumstances, a fixed infrastructure will not be available or it may not be feasible enough to install a new one, like natural disasters, human induced disasters, military or medical situations. It is in such situations that the quick deployment and minimal configuration

DOI : 10.5121/ijnsa.2014.6302

characteristics of MANETs come as an advantage. Due to these reasons, they are widely used in the industry recently.

But these characteristics itself acts as disadvantages to the MANET applications. Lack of centralized infrastructure and management, open environment, random distribution of nodes in space and continuously changing topology makes MANETs vulnerable to the attackers. For example, here the nodes are not much physically protected. So the attackers will easily attack the nodes and those nodes will be used to launch so many kinds of attacks which we will discuss in the next section. Even the routing protocols assume that all the nodes in the network are well behaving and are not malicious. So the attackers can also insert malicious nodes into the network. An intrusion detection system (IDS) specifically designed for MANETs are needed since unlike the traditional networks, MANETs do not have a centralized management system.

Intrusion detection (ID) in MANETs is a lot more complex than in normal wireless networks that are fixed because it is difficult to collect the required data from the MANETs. Also, complexities arise due to the inherent characteristics of MANETs that are mentioned before.

Many more challenges are there which are given below.

- There are no central points where the data collection can be done at.
- MANET routing protocols rely on the intermediate nodes, which in turn makes easy for the attackers to make intrusions.
- As MANETs are mobile, which means there is no fixed topology, the intrusion detection process is more complicated.
- Mobile nodes often will have limited power, limited computing abilities, memory etc. This also makes the ID process complex.

In this paper, we present a survey of certain attacks relevant in MANETs, the respective protection mechanisms and a comparison of the same.

2. MANET ATTACKS

There are many kinds of intrusions or attacks known for MANETs. Like all the attacks, here also the first classification can be done as passive and active attacks as shown in figure 1.

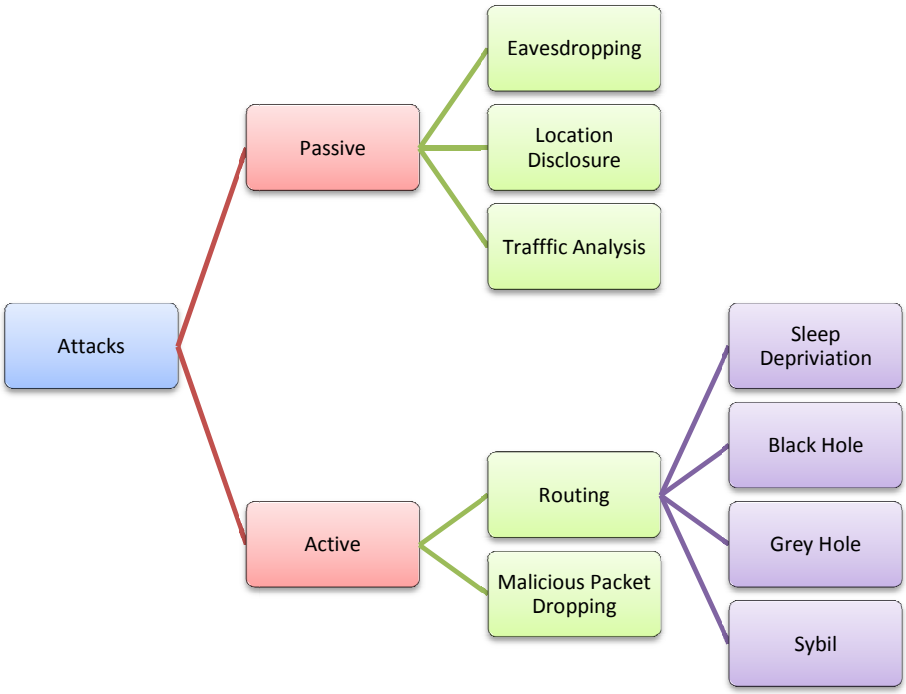

Figure 1. Classification of attacks in the network layer in MANETs.

2.1. Passive Attacks

The working of routing protocols is not at all disturbed during a passive attack but instead aims to collect handy information by analyzing the traffic. The information that comes handy includes the topology of the network, identity, location and other details about the nodes in the network. Described below, are some kinds of passive attacks.

1. Eavesdropping: A major disadvantage of wireless communication aids these kinds of attacks. A communication can be intercieved by any other device which has a transciever and is located within the transmission range. Sometimes encryption will prevent the attackers from getting useful information. But if there is no encryption, then the attackers get the needed information very easily.
2. Traffic Analysis and Location Disclosure: Similar to the eavesdropping approach, the locations of nodes are identified by thorough analysis of the traffic pattern, frquency and amount of transmissions between the nodes. For example in a situation which involves a commanding centre, that centre will be receiving and sending more number of communications. Thus an attacker can easily find the commanding centre by analyzing the communication or traffic pattern.

2.2. Active Attacks

Modification of transmitting, injecting, duplicating, dropping of packets etc will also cause chaos in MANETs. This can be induced by a single attacker or as a collaborative effort of more than one attacker called colluding nodes. They disturb the working of networks and will decrease the performance of the network by a large amount e.g., denial of service attack. This survey focuses mainly on the active network layer attacks. Described below, are some kinds of passive attacks.

1. Malicious Packet Dropping: The route discovery process establishes a route between the source and destination node. To ensure the successful transmission of packets after that, the intermediate nodes in the route must forward the packets. But some malicious nodes may decide to drop the packets. They are also called data packet dropping attack or data forwarding misbehavior.
2. Routing Attacks: Some malicious nodes will utilize the loop holes in the routing algorithms and the distributive or cooperative nature of the algorithms to attack. For e.g., AODV (Ad Hoc On Demand Distance Vector Routing) and DSR (Dynamic Source Routing) [4]. Four main types of routing attacks are discussed below.
    a) Sleep Deprivation Attack: Here a node interacts with other nodes but the interaction is to keep the victim busy.
    b) Black Hole Attack: If the malicious node is chosen as an intermediate node in the route, they may drop the packets instead of forwarding them.
    c) Grey Hole Attack: It is similar to black hole attack. The difference lies in the fact that here the packets are dropped selectively.
    d) Sybil Attack: An attacker node may send control packets using different identities and may create chaos in the routing process.

3. ACKNOWLEDGE BASED TECHNIQUES FOR DETECTING PACKET DROPPING ATTACKS

3.1. Watch Dog

In Watchdog [5], recently sent packets are kept in a buffer and overheard packets are compared with those in the buffer. If a match is found, the packet in the buffer is removed. If a packet remains in the buffer for a long time, a failure tally is incremented for that node which was supposed to forward the packet. A threshold is set, exceeding which the node is considered misbehaving and the source node is notified about that node.

Advantage: It detects misbehavior at the forwarding level as well as the link level.

Disadvantage: Detecting misbehavior in the presence of ambiguous collisions, receiver collisions [6], limited transmission power, false misbehavior and partial dropping is difficult.
Watchdog will work properly only if it has the knowledge about where the packet would be in two hops. Because of that limitation, watchdog works best with a source routing protocol like DSR (Dynamic Source Routing) only.

3.2. PathRater

A rating is maintained for every node in the network that it is aware of. The average of the node ratings is considered and a path metric is calculated. The path which has the highest path metric will be selected, if more than one path is available to a particular destination. Just like watchdog, this must also be implemented on top of a source routing protocol. A neutral rating of 0.5 is assigned to a node at first. It rates itself with a 1.0. The time interval for updating the path metric is set as 200 ms and it increments the ratings on active paths with no misbehavior by 0.01 at periodic intervals. A neutral node can attain a maximum value of 0.8 and a minimum value of 0.0. If a node misbehaves or a link is down, the rating is decreased by 0.05. When the watchdog mechanism is implemented along with path rater, a high negative value of -100 is assigned to nodes that misbehave. A negative value for the path metric indicates that there are one or more misbehaving nodes in that path. If a node is marked as misbehaving due to some temporary fault, it should not be permanently marked so. Therefore, the nodes with

negative ratings should increase the ratings slowly. Another method is to set back the rating to a positive value or 0.0 after a long time.

3.3. TwoAck

The key concept in this technique is that, the node ensures that the packet is received by a node which is two hops away in that route [7]. Just like the normal acknowledgement packets, each node will send an acknowledgement two hops backward called the TWOACK packets. If a node does not receive a TWOACK packet after sending or forwarding a packet, then the next node's link is considered to be misbehaving and that route will not be considered again for routing.
A node will have a list of data packet IDs that are yet to receive a TWOACK acknowledgement packet from a node that is two hops away. Each of the forwarding links will have a separate list in each node. Each item on that list has the following [7]:

- CMIS: Counter which stores the number of misbehaviors detected.
- N2 and N3: The next two hops along that particular route.
- LIST: Data packet IDs that are yet to receive the acknowledgement.
- Whenever a data packet is forwarded along a link, the ID of that packet will be added to the corresponding LIST. When a TWOACK packet is received, the corresponding entry will be deleted. A time period is decided upon and if a packet stays in the LIST for a time more than that specified time out, misbehavior is suspected in that link. If the CMIS count exceeds a particular level or threshold, that link is noted as a misbehaving link and the source will also be informed about the same. Every node will be having a list of misbehaving links and those links will not be chosen for transmitting data packets. This method also distinguishes between actual misbehavior and genuine faults in the network. But the values selected for threshold and time out plays a very important role in deciding the performance of the system.

In order to minimize the traffic created due to these TWOACK packets a selective method can be followed which is the S-TWOACK scheme (Selective-TWOACK). Here the acknowledgement is sent after a certain number of data packets are received and not for each and every packet.
This technique is not affected by ambiguous collisions, attacks using limited transmission power, missed detections or reintroduction of misbehaving nodes [8].

3.4. EAACK – Enhanced Adaptive ACK

This technique employed by Elhadi et.al alleviates three weaknesses of Watchdog viz. false misbehavior, limited transmission power and receiver collision [9]. This technique also introduced the concept of digital signature into intrusion detection. It is an extension work of ACK and selective-ACK (SACK), with misbehavior report authentication (MRA). If the data transmission is not successful and acknowledgements are not received properly, node will switch itself to S-ACK mode. In that mode, malicious nodes even in the presence of receiver collision or limited transmission power will be detected.

The difference from the previous work lies in the fact that the source node has to turn on the MRA mode and confirm the misbehavior rather than believing blindly that misbehavior occurred [9]. Another route to reach the destination is selected or found out by initiating a new route discovery. By sending data packets through that node the malicious node is avoided and the destination node checks whether that particular data packet has already been received. Thus it differentiates between a false report and a trustworthy report. Since this method relies completely on the acknowledgements, all those packets are digitally signed and verified to ensure reliability.

3.5. SCAN – Self organized Network Layer Security

The approach employed in SCAN [10] uses the same technique for protecting both the routing and data packets. The two important features of this technique are:

- Collaboration with the local nodes: Neighboring nodes
- Cross validation of information: The results found by each node will be cross validated by the nodes.

These two features make this technique a self organized one. A suspected node will be removed from the route only when a particular number of neighboring nodes reach a consensus. Thus this technique employs a distributed consensus mechanism. The chances of inaccurate results from a single node are avoided by following this method. Thus there is a very high probability of removing malicious nodes and reduced probability of wrongly removing a legitimate node.

Token mechanism is used in this approach which includes token renewal and token revocation. Each node must have a valid token with it in order to participate itself in a transmission. They can renew the token once the present token expires. The token of an accused node will be revoked by all other nodes. All these processes are done in a collaborative manner to prevent forgeries. Also, these tokens will be protected by means of public key cryptography techniques. No node is superior to any other node. The secret key is shared between; say k, number of nodes. Thus this technique avoids attacks with less than k colluding attackers. A token revocation list (TRL) is maintained, based on which the token requests are processed [10]. When the node gets k TREP (Token Reply) packets, they are combined into a single token. A credit strategy is employed in this approach whereby well behaving nodes are given more token life time and thus their token renewal overhead is lesser. The packet drop detection method used in this technique is similar to the watchdog technique discussed before.

3.6. Black Hole attack Detection using Topology Graphs

Elmar and Marko proposed a technique to detect black hole attacks in tactical MANETS called Topology Graph based Anomaly Detection (TOGBAD) [11]. This is based on the Optimized link state routing protocol (OLSR). The supervising nodes are used as the centre for topology graph creation and misbehavior checks. The centralized working of this technique can be considered as a disadvantage when employed in normal MANETs.

HELLO messages in OLSR will contain the information about the neighboring nodes local links etc. Thus here, the number of neighbours in the HELLO messages is compared with that in the topology graph and a difference indicates misbehavior. A cluster based anomaly detector from the works [12] and [13] have been used in this technique. The round length in the detector has to be fixed as greater than the HELLO message interval. Thus there exists a trade off situation between precision and resource consumption. Each node will extract the number of neighbours from HELLO message and will send that information to the central supervising node. Misbehavior detection is done by fixing a threshold value and if the difference calculated is more than that threshold, then a misbehavior is suspected. Fixing the threshold value is a difficult task, which has to be based on lots of metrics.

3.7. Black Hole Attack Detection using Dynamic Learning Method

Kurosawa et.al. introduced a technique that detects misbehavior with very good accuracy by employing a training method and updating the training data in periodic time intervals [14]. This technique also adapts to the changing network environment by defining the normal state

adaptively. A multidimensional feature vector is defined in order to express the state of the network. The state of the network is expressed using the number of RREQ (Route Request) messages that are sent out, number of RREP (Route Reply) messages received and the average of difference of destination sequence number in each of the time slots and the one that is stored in the list. The destination sequence number indicates how much fresh the routing data in the message from the source is.

For anomaly detection, the network state in a time slot is expressed with a three dimensional vector. Normal states will be seen as together in the feature space. Abnormal state will be the data that is scattered and is away from the normal state. Using training data set for N time slots, the mean vector is calculated. After that the distance of this mean vector from the input data sample is found out. If the distance calculated is larger than a threshold value that is set, then that is considered an attack. The threshold value can be extracted from the learning data set [14]. It is an advantage of this system that it continues learning the state of the network.

3.8. LIP: Light Weight Interlayer Protocol

Hsu, Zhu and Hurson proposed a method that is efficient against packet injection attacks in MANETs. It does not have the overhead of calculating the digital signatures for all the packets [15]. This technique is also efficient against attacks involving impersonation techniques. This follows an inter layer design by which it achieves independence and transparency. This can be implemented as a security layer in between the network and data link layer.

In this technique, a node will compute only one message authentication code (MAC) for each message that is sent. That MAC key is shared with the neighbours. It is evident that, since the keys have a symmetric nature, it is possible for a malicious node to impersonate another legitimate node. To prevent this impersonation attack, some techniques are used in this method.

- Using one time cluster keys: A cluster key will be used by a node only once. Thus an attacker cannot use the same key for forging. Hash functions that have the one way property is used to get the one time cluster keys.
- Random verification of neighbourship: A node responds with a CHALLENGE message at probability Pc. If the other node is able to hear this message, it will respond with an acknowledgement message along with a FLAG. A true value of FLAG indicates that the node has really forwarded the packet. Since the shared key is used to encrypt the messages, impersonating attacker cannot forge these messages. But the value of Pc will be a tradeoff between performance and security. Thus Pc is fixed based on the node density estimate of the network.

A location aware version of this verification technique further reduces the overhead by not initiating verification when the nodes are highly likely that they are neighbors.

3.9. Defence Against Grey Hole Attacks

Xiaopeng and Wei introduced a mechanism to detect grey hole attacks for the DSR routing protocol. An aggregated signature algorithm is used in this approach by each node to produce an evidence for packets forwarded [16]. A check up algorithm is used to detect packet dropping. A diagnostic algorithm is used by the source node to trace the misbehaving node. This proposal was modified in their next work [17], by introducing a Distributed Certificate Authority (DCA) to update the information about key management.

3.10. Packet Drop Detection

This is based on the principle of conservation of flow in a network, i.e., all packets sent to a node which is not meant for that node must go out of that node [18].

4. INTRUSION DETECTION SYSTEMS

Intrusion detection systems are not specific for any attacks. They are designed in such a way that they are able to tackle more than one kind of attack.

Anomaly Based Intrusion Detection systems find a model of the normal state of the network and compare it with the present state of the network. Deviations indicate an attack. The two phases involved are training phase, with the normal model and the testing phase, which uses mathematical or statistical methods. Neural network algorithms can also be included in this kind of detection systems for training. But they may generate false alarms.

Different probabilistic techniques like chi-square test, Markov chain, Decision tree(Pattern Recognition Technique) etc is used on the same training data and same testing data for deciding which properties are important to intrusion detection [19]. They worked on a sample of normal and intrusion denoting computer audit data. After comparing all the techniques, they have concluded that chi-square test can be used based upon frequency property and Markov model based upon ordering property are good for detecting intrusion.
Knowledge Based Intrusion Detection (KBID) systems will have a known database of signatures that correspond to known attacks. Those known signatures are searched for to detect intrusions. Expert systems that maintain the signatures as rules can also be used. But those attacks which are not available in the database will not be detected and thus, the database has to be kept updated, which is a tedious job.

In Specification Based Intrusion Detection (SBID) systems, constraints are specified, based on which the operations are monitored and attacks are detected. This kind of detection can be done based on the syntax or the semantics of the operations. M. Jahnke et.al. uses finite state machines for specifying the normal routing behavior in AODV routing protocol and the network is monitored for run time violations in a distributed manner [20]. These kinds of specification detections do not detect the intrusions but the effects of intrusion. This technique is not limited to the known attacks. The request-reply flow is monitored using distributed Network Monitors (NM).A finite state machine is employed in these network monitors for detecting incorrect request and reply packets. Inconsistent sequence number or hop count will direct the state machine to the suspicious state. This technique is also able to detect spoofing because the network monitor also maintains a mapping between the IP address and MAC address of every node in the network. A session tree is used in their algorithm which is constructed when a request is received and processed during the reply. This technique is found to be effective against attacks like man in the middle attack, forging sequence numbers and tunneling attack that are examples of aggregated attacks.

5. COMPARISON

The techniques discussed above are compared in Table I below. They are analyzed based on the routing overhead and packet delivery Ratio. Most of the techniques that exist are based on a particular routing protocol. But that reduces the generality of these methods. More than one technique will have to be implemented on a single MANET and that would increase the complexity of the system. Network traffic, processing overhead etc will increase. Researches on a

more general attack detection mechanism for MANETs that can be implemented on top of MANETs with any routing protocol is very rare. Interrelations between the different detection mechanisms should also be considered when implementing them in MANETs.

Table 1. Comparison based on routing overhead and packet delivery ratio

Technique	***Advantages***	***Disadvantage***
WATCHDOG AND PATHRATER	Increase throughput by 17% in a network with moderate mobility. With extreme mobility,network throughput is increased by 27%.	Detecting misbehavior in the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior and partial dropping is difficult.
TWOACK	With 40% misbehaving nodes. Packet delivery ratio - 90%.	Overhead increased to 7%
EAACK	MRA scheme aids in detecting false misbehaviour report.	RSA scheme uses more battery power and performance decreases than DSA(Digital Signature Algorithm) scheme
SCAN	Packet Delivery Ratio increases by a factor up to 150% even if 30 % nodes are malicious	.Overhead Steadily increases as there are more malicious nodes in the network and as node mobility increase.
TOGBAD	Packet delivery ratio stays at nearly 90 %. Average drop is about 60 % with black hole attack.	Centralized system. Attacks against TOGBAD itself have not been studied. Black hole may change the topology graph creating messages as well
DYNAMIC LEARNING	Can adapt to the changing network conditions	Can be used only under AODV routing protocol
LIP	Packet delivery Ratio close to 1.0 even though it goes down slightly when the node mobility increases. Low bandwidth overhead.	Overhead increases with mobility of nodes.

6. CONCLUSIONS

The fast mobility and geographically distributed nature of MANETs makes it more vulnerable to attacks, esp., network layer attacks. In this paper, we have presented a survey of important network layer attacks and have reviewed some of the important misbehavior or intrusion detection mechanisms existing. Some techniques are specific for certain attacks while some others are able to deal with a variety of attacks.

Even though highly effective detection mechanisms have been proposed, intruders often use new methods to attack the networks. Due to that, devising new techniques for intrusion detection based on the newly emerging attacks is a very important area of research. The detection mechanisms also have to be protected. Thus this is a never ending research area.

REFERENCES

[1] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.

[2] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[3] 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.

[4] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[5] S. Marti, T.J. Giuli, K.Lai and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks",(2000), Proceedings of International Conference on Mobile Computing and Networking, pp 255- 265.

[6] J. Jubin and J. Tornow. The DARPA Packet Radio Network Protocols. In Proceedings of the IEEE, 75(1):21-32, 1987.

[7] Balakrishnan, K. ; Jing Deng ; Varshney, P.K. , "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks",(2005), Wireless Communications and Networking Conference, IEEE.

[8] K. Balakrishnan, "Prevention of Node Selfishness in Mobile Ad Hoc Networks", M.S. Thesis, Department of EECS, Syracuse University, Syracuse, NY, USA, August 2004.

[9] Elhadi M. Shakshuki, Nan Kang, Tarek R. Sheltami "EAACK—A Secure Intrusion-Detection System for MANETs", (2013), ieee transactions on industrial electronics, vol. 60, no. 3.

[10] H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks", (2006), IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 261-273.

[11] E.Padilla, N.Aschenbruck, P.Martini, M.Jahnke and J.Tolle, "Detecting Black Hole Attack in Tactical MANETs using Topology Graph", (2007), Proceedings of IEEE Conference on Local Computer Networks.

[12] Jahnke, J. T¨olle, M. Bussmann, and S. Henkel, "Components for Cooperative Intrusion Detection in Dynamic Coalition Environments", (2004), NATO/RTO IST Symposium on Adaptive Defence in Unclassified Networks.

[13] J. T¨olle, M. Jahnke, N. gentschen Felde, and P. Martini, "Impact of Sanitized Message Flows in a Cooperative Intrusion Warning System", (2006), 25th Military Communications Conference (MILCOM 2006).

[14] S. Kurosawa and A. Jamalipour, "Detecting Blackhole Attack on AODVbased Mobile Ad Hoc Networks by Dynamic Learning method", (2007), International Journal of Network Security, Vol.5, No.3, pp 338-345, November.

[15] H. Hsu, S. Zhu and A. R. Hurson, "LIP: a Lightweight Interlayer Protocol for Preventing Packet Injection Attacks in Mobile Ad Hoc Networks", (2007), International Journal of Security and Networks, Vol. 2, Nos. 3/4, pp. 202 - 215.

[16] G.Xiaopeng and C.Wei, "A Novel Grey Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", (2007), IFIP International Conference on Network and Parallel Computing.

[17] C. Wei, L. Xiang, B. Yuebin and G.Xiopeng, "A New Solution for Resisting Grey Hole Attack in Mobile Ad Hoc Networks", (2007) IEEE Conference on Communication and Networking, China.

[18] O.F. Gonzalez-Duque, G. Ansa, M. Howarth and G. Pavlou, "Detection and Accusation of Packet Forwarding Misbehaviour in Mobile Ad hoc Networks", (2008), Journal of Internet Engineering, Vol.2, No.8, pp 181-192.

[19] N.Ye, X.Li, Q.Chen, M.Emran and M.Xu, "Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data", (2001) IEEE Transactions on Systems, Man, and Cybernetics, Vol. 31, No. 4, July.

[20] J. T¨olle, M. Jahnke, N. gentschen Felde and P. Martini, "Impact of Sanitized Message Flows in a Cooperative Intrusion Warning System", (2006), Proceedings of the 25th Military Communications Conference (MIL-COM).

Authors

Punya Peethambaran is an M tech Student at Sree Chitra Thirunal College of Engineering under Kerala University, Trivandrum, Kerala. Punya Recieved her B tech degree in Computer Science at Cochin University College of Engineering in 2011. She has worked in the industry for one year, her interest domain is security, wireless network, intrusion tolerance and cloud computing.

Dr. Jayasudha J. S. is the head of the department at the Department of Computer Science and Engineering, Sree Chitra Thirunal College of Engineering,Kerala University.