IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

Probabilistic and Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks

Sureka .M[1], Kalaivani .K[2], Sridharani .S[3], Ieshwarya .R[4]

Student Member, Department of Computer Science and Engineering, Arasu Engineering College,

Kumbakonam, Tamil Nadu, India[1, 3, 4]

Staff Member, Department of Computer Science and Engineering, Arasu Engineering College,

Kumbakonam, Tamil Nadu, India[2]

Abstract: A mobile ad hoc network (MANET) is a self-organized collection of mobile nodes which communicate with each other without the help of any fixed infrastructure or central coordinator. A node intending to communicate with another node that is not within its communication range, takes help of intermediate nodes to relay its message. The topology of the network dynamically changes over time as nodes move about, some new nodes join the network or few other nodes disengage themselves from the network. Intrusion Detection Systems (IDS) are used in MANETs to monitor activities so as to detect any intrusion in the otherwise vulnerable network. Communication has become very important for exchanging information between people from, to any time via mobiles. MANET is a group of mobile nodes that form a network independently of any centralized administrator for communication. Since those mobile devices are battery operated and extending the battery lifetime has become an important aim. Most of the researchers have recently started to consider Power –aware development of efficient protocols for MANETs. Also the nodes in the network are moving if a node moves out of the radio range of the other node, the link between them is broken. so we presented an original solution called IMAPC – MAC Protocol(Improved Autonomous Power Control) In this paper, an efficient scheme for analyzing and optimizing the time duration for which the intrusion detection systems need to remain active in a mobile ad hoc network is presented. A probabilistic model is proposed that makes use of cooperation between IDSs among neighborhood nodes to reduce their individual active time. Usually, an IDS has to run all the time on every node to oversee the network behavior. This can turn out to be a costly overhead for a battery-powered mobile device in terms of power and computational resources. Hence, this work is to reduce the duration of active time of the IDSs without compromising on their effectiveness.

Keywords: Adhoc Networks, Intrusion Detection, Energy efficiency, MANET, IMAPC-MAC protocol.

I. INTRODUCTION

A MANET can be defined as a collection of wireless mobile nodes that form a dynamically changing network, without using any infrastructure or centralized administration. Such a network is created as the nodes communicate and each other, with each having capability to act as a whenever necessary. The network topology, MANET is a connection session can be established either through a single-hop transmission if the communication pairs are close enough or through multi hop relay by intermediate nodes. Different from other types of wireless networks, a MANET does not need fixed infrastructure such as base stations or access points.

The rapid progress of information technology brings with itself more sources of information and more vulnerability to the available information. Protecting the networks from intrusion seems to be a major challenge in the current scenario. Computer networks are usually protected against attacks by a number of access restriction policies that act as a coarse grain filter. Intrusion detection systems (IDS) are the fine grain filter placed inside the protected network, looking for known or potential threats in network traffic and/or audit data recorded by hosts.

The frequency of intrusions has increased to a large extent during the recent years, hence maintaining an effective intrusion detection system has become mandatory. Intrusion detection systems analyze packets to identify if they are legitimate. This process is complicated due to the generation of a huge number of packets in networks. Not all packets can be examined. Further, attacks differ in styles and operational levels. Hence a static intrusion detection system does not suffice. This mandates the need for a dynamic and learning intrusion detection system that can identify anomalous packets effectively in a huge network without hindering the process flow. With the rapid advances in research on wireless technology, wireless ad hoc networks have become an attractive choice for both commercial and military applications. In these networks, security and energy efficiency are of primary concern. [10], [11], are usually deployed in the network to detect malicious activity.

Although several IDS systems are available, the common objectives of these systems are to reduce the amount of false alarms, and to recognize new attacks in order to increase detection ratio. In this paper, the concentration is

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

on detecting known and unknown attacks in fast networks in order to mitigate the influence of the attack by shrinking the time gap between the real attack and its detection.
The proposed system is dedicated to detect intrusions on a network by using anomaly intrusion detection approach. This approach is used to detect the known and novel attacks in traffic network.
The contributions of this project are summarized as follows:

1. A novel technique, based on a probabilistic model, to optimize the active time duration of intrusion detection systems (IDSs) in a MANET. The scheme reduces the IDSs' active time as much as possible without compromising on its effectiveness.
2. Considerable saving in energy and computational cost is achieved using the proposed technique of optimizing the active time of the IDSs while maintaining the performance of the IDS.
3. The proposed scheme uses local information, thus making it distributed and scalable. Moreover, it works on both static and mobile networks.

II. RELATED WORKS

Watchdog and Path rater S. Marti, K. Lai, ET al has proposed this scheme to detect packet dropping and misbehaving nodes in MANET [1]. In watchdog scheme, node overhears to his neighbor about status of packet handed by him to that particular neighbor. To check for misbehavior, node maintains the copy of packet forwarded in his buffer then he promiscuously checks whether adjacent node modify, drop or simply forwards the packet. If adjacent node forwards the packet as it is then copy of packet maintained in buffer is removed. If packet remains in buffer for a time greater than timeout period then that packet flagged as dropped or modified and corresponding neighbor marked as suspicious. If number of violations made by adjacent node exceeds certain threshold then that node marked as malicious. Path rater component rates different nodes according to their reliabilities and helps to avoid route through malicious nodes. Watchdog scheme fails in situations like receiver collision, ambiguous collision, limited transmission power, false misbehavior report, multiple colliding nodes and partial dropping.

A. TWOACK

This scheme is not modification to watchdog but it is successful in removing three important weaknesses of watchdog which are receiver collision, limited transmission power and ambiguous collision [2]. TWOACK can be implemented as an additional functionality into the existing routing protocols like DSR. It uses new acknowledgement packet termed as TWOACK to detect misbehaviors and it will be sent in opposite direction of normal route for two hops.

B. AACK (Adaptive Acknowledgement)

Sheltami et al. [3] proposed a new scheme AACK based on TWOACK. It is also network layer scheme similar to TWOACK but aimed at reducing network overhead occur in TWOACK scheme. This scheme uses two modes for operation first end to end acknowledgement and other TACK (similar to TWOACK). In absence of packet dropping, node continues to work in first mode. Otherwise system switches to TACK mode and continue to remain in that node till first packet reaches to destination and switches back to end to end acknowledgement mode. Thus AACK able to remove second shortcoming of TWOACK scheme stated above by partial detection for malicious nodes.

C. Enhanced Adaptive Acknowledgement (EAACK)

Working of watchdog, TWOACK and AACK is based on acknowledgement based scheme. So it is crucial to know whether acknowledgement packets are authentic and valid. To address this problem E. M. shakshuki et al. have proposed new scheme EAACK [4] that uses digital signatures to ensure integrity and authenticity of acknowledgement packets. EAACK successful in removing three weaknesses of watchdog, namely false misbehavior report, limited transmission power, and receiver collision. TWOACK and AACK schemes are vulnerable to false misbehavior report attack. EAACK consist of three modes ACK, S-ACK and misbehavior report authentication (MRA). ACK is end to end acknowledgement based scheme help to reduce network traffic. In S-ACK mode, three consecutive nodes in network work to find out misbehaving nodes in the network. S-ACK mode helps to remove receiver collision and limited transmission power weaknesses of watchdog. EAACK do not immediate trust on the misbehavior report and switches to MRA mode. In this mode, node sends MRA packet to destination on other route than currently used route. If destination node have already received reported packet then report marked as misbehavior report otherwise report is trusted.

III. METHODOLOGIES

The proposed system is dedicated to detect intrusions on a network by using anomaly intrusion detection approach. This approach is used to detect the known and novel attacks in traffic network.

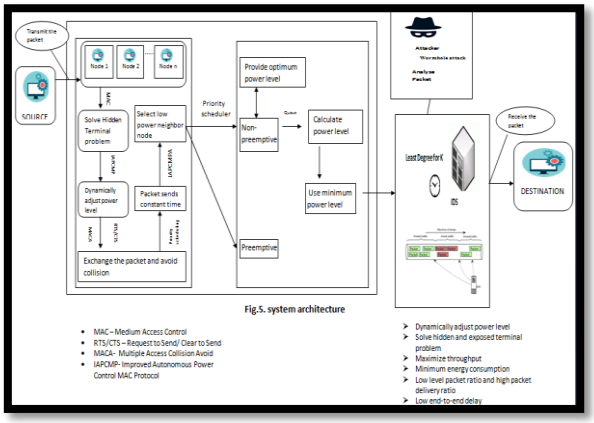


Fig 1: Proposed Energy consumption based on IDS in MANET

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

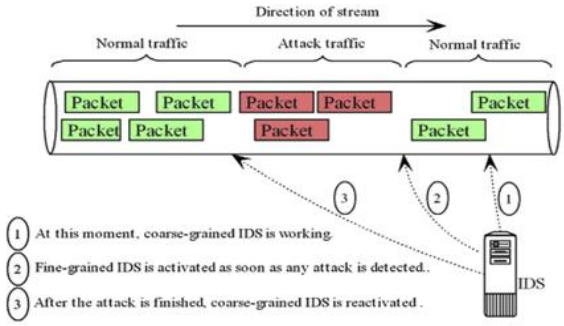


Fig 2: Detection of Intruders in Fine-grained IDS

The main contributions of this paper are summarized as follows:

1. A novel technique, based on a probabilistic model, to optimize the active time duration of intrusion detection systems (IDSs) in a MANET. The scheme reduces the IDSs' active time as much as possible without compromising on its effectiveness.
2. Considerable saving in energy and computational cost is achieved using the proposed technique of optimizing the active time of the IDSs while maintaining the performance of the IDS.
3. The proposed scheme uses local information, thus making it distributed and scalable. Moreover, it works on both static and mobile networks.

A distributed scheme to determine the ideal probability with which each node has to remain active (or switched on) so that all the nodes of the network are monitored with a desired security level. The main aim of this proposed system is,

1. It reduce the IDS's active time at each node in the network.
2. The effectiveness of the IDSs in the network is not compromised while using the proposed scheme, rather, there is considerable reduction of energy consumption in each of the nodes that increases the network lifetime significantly.

0verall, there are four subsytem in our proposed system to detect intrusions on a network, including Network Formation, AODV Routing, Intrusion Detection, IMAPC MAC Protocol(Saving energy).

A. Network Formation

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Ssuch networks may operate by themselves or may be connected to the larger Internet.

B. AD-HOC On-Demand Distance Vector Routing (AODV) Protocol

AODV is an on-demand routing protocol designed for operation of mobile ad hoc network. Protocol provides self starting, dynamic, loops free, multi-hop routing. Protocol allows mobile nodes to establish routes quickly for new destinations as well as to respond to changes in network topology and link failures as only affected set of nodes are notified. Nodes do not maintain routes to the destinations that are not in active communication. New routes are created on demand. It means control packets are broadcast when needed and hence eliminate the need for periodic broadcast of routing updates.

AODV protocol works in two phases,

a) Route discovery process and

b) Route maintenance process.

Route discovery process uses Route Request (RREQs) and Route Reply (RREPs) messages. The routing messages contain information only about the source and the destination. When a route to destination is needed, the node broadcasts a route request (RREQ) packet to its neighbors to find the optimal path.

RREQ message contains route request broadcast ID, Destination IP Address, Destination Sequence Number, Source IP Address, Source Sequence Number and Hop Count. Sequence number is used for route freshness, loop prevention and faster convergence. When a node sends any type of routing control message like RREQ/RREP, it increases its own sequence number. Every node should include the latest sequence number for the nodes in the network in its routing table. It is updated whenever a node receives RREQ, RREP or RRER related to a specific node. Hop count represents the distance in hops from the source to destination. Each node receiving the RREQ message sets up reverse path back to the sender of the request so that RREP message can be unicast to that sender node from the destination or any intermediate node that satisfy the request conditions. Upon receiving the route request message, the intermediate node forwards the RREQ message until a node is found that is the destination itself or it has an active route to the destination with destination sequence number greater than or equal to that of RREQ. This node replies back to the source node with a route reply message RREP and discards the RREQ. If the intermediate node receives RREQ with 'G' flag set, it must also uncast gratuitous RREP to the destination node. RREP contains Destination IP Address, Destination Sequence Number, Originator IP Address and Lifetime. Forward links are setup when RREP travels along the reverse path. Once the source node receives the route reply, it establishes a route to the destination and sends data packet along forward path set-up.

Route maintenance is performed with two additional messages: Hello and RRER messages. Each node broadcast Hello messages periodically to inform neighbors about its connectivity. The receiving of Hello message proves that there is an active route towards the originator. When a node does not receive HELLO message within time period from a neighbor node then it detects that a link

DOI 10.17148/IARJSET.2016.31103

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

to that neighbor node has broken then it generates route error message (RRER). RRER message indicates those destinations that are unreachable, their IP address and destination sequence number. In order to inform the link failure information, each node maintains a precursor list for each routing table entry containing the IP address of set of neighboring nodes that are likely to use it as a next hop towards each destination. On receiving this RRER, each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. In addition to these routing messages, the route reply acknowledgment (RREP-ACK) message must be sent by sender node of RREQ in response to a RREP message with the 'A' bit set. This provides assurance to the sender of RREP that the link is bidirectional.

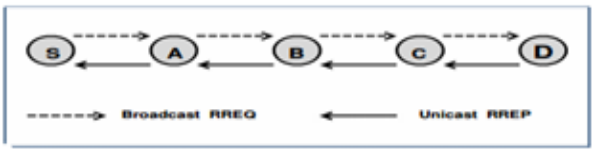


Fig 3: The routing message exchange in AODV

C. Intrusion Detection

Consider a network of wireless nodes, each having an intrusion detection system (IDS) that is responsible for detecting malicious activities within its neighborhood. Assume that a mobile node is watched for malicious activities by all its neighbors (nodes within its radio range) using these IDSs. Hence, by neighbor, i.e., 1- hop neighbor throughout the rest of the paper. At any instant of time, all or some of the k neighbors may detect the malicious activity of node a depending upon the detection rate of the IDS components on them. More importantly, the neighbors spend their valuable computational resources and energy while monitoring node a all the time. However, it may not be required to keep the IDS running on each node all the time. The proposed system attempt to reduce this redundancy, thereby saving therefore - mentioned resources.

The assumptions that are made are summarized as follows:

1. Each node is equipped with an IDS component.
2. The IDS monitors the traffic of its neighbors all the time.

1. Least Degree for k

Each node (say M) initiates this algorithm to determine the probability with which it has to monitor its neighborhood. In step 1, M broadcasts the message Send-Degree.

This message is limited to only one hop. In step 2, the neighbors of M reply back with their respective degrees. In step 3, the least of these degrees is assigned to k in the formula, and the minimum monitoring probability of M ($p^M min$) is calculated.

Algorthim LDK

Step 1: Each node M broadcaste a message of type Send-Degree to its neighbors asking them to send their degree.

M→broadcast(SendDegree)

Step 2: On receipt of the Send Degree message in step 1, each neighbor node, B of M replies to M a Reply Degree message.

B→M (Reply Degree)

Step 3: On receipt of each Reply Degree message in Step 2, M does the following.

i. For each message do degree = Reply Degree;
ii. K = Minimum(degree);
iii. If l>K then P_M^{min} =1otherwise P_M^{min} is assigned the minimum value of P(where l is the desired security level of neighbor,T+ε = 1, ε is a very positive number) such that

$$\sum_{i=1}^{k} \binom{x}{y} p^i (1-p)^{k-i} \geq T$$

In step 2 of LDK, a malicious neighbor may send false degree information to M and try to disrupt the algorithm. However, LDK is resilient to such an attack under the following assumption. It is assumed that a malicious neighbor of M would like $p^M min$ to be as less as possible so that the chance of being detected is reduced. It cannot change its security level and thus to be monitored with a low monitoring probability, it can only send a high degrees to M in step 2.

Since the minimum degree of the neighbors is chosen by M in step 3 to determine the value of $p^M min$, the high degree sent by the malicious neighbor will most likely not be chosen. Even if several malicious neighbors collude and report an inflated high degree, if there is at least one honest neighbor which reports correctly, the honest neighbor's degree will be chosen as the minimum degree (in step 3) and $p^M min$ will be correctly calculated.

D.IMAC-MAC Protocol

1) Estimation of Power Level:

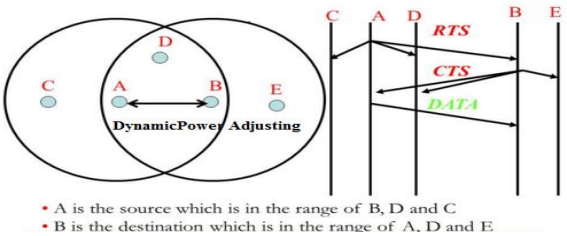


Fig 4: Dynamic adjusting the power

$$E_s = \frac{\sum_{i=0}^{n} T_p + \sum_{j=0}^{m} R_p}{\sum_{k=0}^{l} D_p} \qquad t_s, t \geq o, p > 0$$

Where,

T_p - Transmit the total packet.
R_p - Receiving packet from source.
D_p - Retransmitting the packet.

2. POWER UTILIZATION:

$$\frac{S'}{E'_C} = \frac{Q[i]}{\sum_{i=1}^{N} P_i^r T_i^r + \sum_{j}^{M} P_j^r T_j^r} * \beta(OP)$$

Where,

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

S' - Total number of successful data bits sent between source and destination
E_C' - Total energy consumption in the network
N - Total number of packets sent(including control packets) for duration of the simulation (from all nodes).

3.IAPCMAC Protocol:

Power saving schemes has been proposed to minimize energy consumption in MANETs. These schemes fall under three main categories:

- Transmission power control
- Low power mode
- Power saving

4. Transmission Power Control:

Transmission power control is adjusted according to desired criterion. Power conservation is to reduce the amount of power used by individual nodes and by the aggregation of all nodes to transmit data through the ad hoc network. Two components determine the cost of communication in the network. First one is direct node to node communication or transmission. The transmission rate can be adapted by the sender. Second is forwarding of data through the networks. In the first case we can use the power control techniques to conserve the power. Whereas in the second case we can use the energy efficient power control scheme.

Current technology supports power control by enabling the adaptation of power levels at individual nodes in an ad hoc network. Since the power required transmitting between two nodes increases with the distance between the sender and the receiver, the power level directly affects the cost of communication.

The power level defines the communication range of the node and the topology of the network. Due to the impact on network topology, artificially limiting the power level to a maximum transmit power level at individual nodes is called topology control.

5. Low Power Mode:

IAPCMAC, an energy-conserving multi-access protocol for MANETs using busy tones where radios that are not actively transmitting or receiving a packet power themselves off in a manner that does not influence the delay or throughput characteristics of the protocol.

The node with the goes to idle state and it is considered as an off state, such as the power level not decrease. This protocol only saves power with increasing the overall network throughput.

6. Power Saving:

1. ON/OFF mechanism of nodes: - In this, any node can power off itself when there is nothing to do for that node or if any neighboring node is transmitting at that time. A node can power down itself for without affecting the performance of neighbor nodes.

2. Power saving mechanism:- In this, control messages are sent using maximum power available and data messages are sent using minimum or sufficient power required for transmission.

7. Optimum Transmission Power:

Calculate the optimal values for the following:

$$OP = \sum_{i=1}^{n} P_i(t_c)(r_c) * Q[i]$$

Where,

OP- Optimal value of transmission power
t_c - Optimal transmission time
r_c - Optimal transmission rate

8. Scheduling Phase:

This priority scheduling gives each process a priority well defined. This way every process has its own priority on which will depend if it is going to be run or wait. The first one to run is going to be the process with highest priority, while others will wait for their turn. It schedules the data packets based on its priority index. The priority index is attached to the header of the data packets. Its value is based on the queue length of the node, data rate of the source (which is normalized with respect to channel capacity), and expiry time of the packet. This scheduler favors data packets as compared to control packets. It aims to improve the average throughput by quickly delivering packets with greater remaining hops or distance.

9.Priority Queue:

Priority queue is for selecting flows based on the priority. Here the priority is assigned for flows which contain loss number of slots, optimal transmission rate of flow and optimal transmission power of flow. All the flows are queued based on the priority. The flows are entered into the queue based on the priority which they have

F1	F2	F3	F4	----------		

The flows will be queued based on their priorities. After getting the input priorities queue we will apply the non-preemptive scheduling algorithm. We will get the optimal transmission rate value and the optimal transmission power value.

10. Calculate the queue length:

The percentage of Queue length α, β, and γ for X, Y and Z queues respectively are calculated as in following equation,

$$\alpha = \frac{Q[i]_{lx}}{Q[i]_{lx} + Q[i]_{ly} + Q[i]_{lz}}$$

$$\beta = \frac{Q[i]_{ly}}{Q[i]_{lx} + Q[i]_{ly} + Q[i]_{lz}}$$

$$\gamma = \frac{Q[i]_{lz}}{Q[i]_{lx} + Q[i]_{ly} + Q[i]_{lz}}$$

Where,

$Q[i]_{lx}$ - Queue length of X (HP – Higher priority)
$Q[i]_{ly}$ - Queue length of Y (MP – Medium priority)
$Q[i]_{lz}$ - Queue length of Z (LP – Lower priority)

We decide the number of packets to be each queue based on their access ratio given in equation

$$w0\alpha : w1\beta : w2\gamma$$

Where,

w0, w1, w2 are the user defined weights assigned for X(HP), Y(MP) and Z(LP). α is the percentage of

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

X(HP) packets, β is the percentage of Y(MP) packets and γ is the percentage of Z(LP) packets waiting in their respective queues. When the traffic is dominated by Y(MP) or Z(LP) packets, the queue length of Y(MP) and Z(LP) may increase and thus the access ratio of X(HP) packets.

IMAPC-MAC Protocol Algorithm
1. Start
2. Define $P_i=\{P_1,P_2,P_3\ldots\ldots\ldots P_n\}$ (set of flow),

$$Q[P_i] = \text{priority queue}$$

3. N – Number of packet allocated for each flow
4. Calculate the queue length using by the non-preemptive technique
5. Transmitter power is estimate using priority scheduling
6. Add that flow to the queue $Q[P_i]$
7.

$$OP = \sum_{i=1}^{n} P_i(t_c)(r_c) * Q[i]$$

Where,
OP - Optimal value of transmission power
t_c - Optimal transmission time
r_c - Optimal transmission rate
8. Transmission cycle is finished.
9. End

IV. PERFORMANCE EVALUATION

In this section we discuss Algorithm LDK, Improved autonomous power control MAC-Protocol in MANET performance.

A. Throughput:
It is defined as the total number of packets delivered over the total simulation time.
Mathematically, it can be defined as:

Throughput= N/1000

Where,
N is the number of bits received successfully by all destinations.

B. End to end delay:
The average time it takes a data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination. Mathematically, it can be defined as,

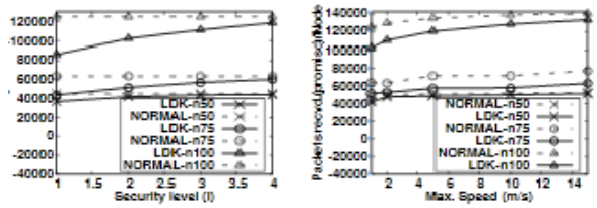
Avg. EED=S/N

Where,
S is the sum of the time spent to deliver packets for each destination,
N is the number of packets received by the all destination nodes.

C. Packet delivery ratio:
Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined as:

PDR= S1÷ S2

Where,
S1 is the sum of data packets received by the each destination.
S2 is the sum of data packets generated by the each source.



(a) M=5, P=1m/sec (b) M=5, l=2

Fig 5. No of packets recvd(promisc)per node

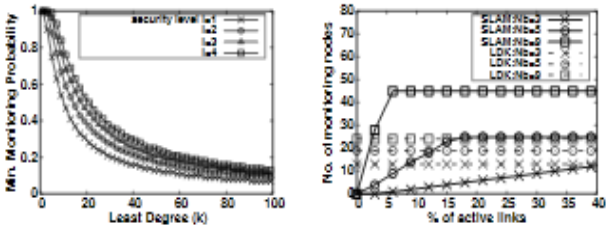


Fig 6. Effect of Least degree of neighbors(k) and comparison of SLAM

TABLE I EFFICTIVENESS/ENERGY SAVING AT VARYING SECURITY LEVEL

N	l	DR (normal)	DR (LDK)	FDR (normal)	FDR (LDK)	engy. (normal)	engy. (LDK)	pkts rcd. (normal)	pkts rcd. (LDK)
50	1	0.968	0.959	0.0046	0.0052	5.804	4.743	45268	37007
	2	0.943	0.945	0.0026	0.0023	5.804	5.401	45268	42078
	3	0.910	0.900	0.0020	0.0011	5.804	5.603	45268	43779
	4	0.852	0.858	0.0015	0.0014	5.804	5.688	45268	44458
75	1	0.937	0.936	0.0291	0.0257	8.065	5.527	63730	45609
	2	0.912	0.895	0.0173	0.0159	8.065	6.560	63730	51701
	3	0.888	0.887	0.0148	0.0152	8.065	7.221	63730	56998
	4	0.851	0.838	0.0130	0.0159	8.065	7.626	63730	60269
100	1	0.776	0.774	0.1016	0.1099	13.199	9.080	125027	86282
	2	0.675	0.680	0.0725	0.0453	13.199	10.790	125027	102505
	3	0.618	0.600	0.0603	0.0528	13.199	11.738	125027	111298
	4	0.561	0.514	0.0493	0.0444	13.199	12.501	125027	118748

TABLE II EFFICTIVENESS/ENERGY SAVING AT SPEED

N	P	DR (normal)	DR (LDK)	FDR (normal)	FDR (LDK)	engy. (normal)	engy. (LDK)	pkts rcd. (normal)	pkts rcd. (LDK)
50	1	0.943	0.945	0.0026	0.0023	5.804	5.401	45268	42078
	2	0.928	0.932	0.0049	0.0065	6.462	6.108	50376	47647
	5	0.913	0.916	0.0076	0.0061	6.435	6.199	50653	48708
	10	0.896	0.890	0.0084	0.0103	6.500	6.2914	51649	50020
	15	0.834	0.842	0.0228	0.0155	6.581	6.429	52526	51277
75	1	0.912	0.895	0.0173	0.0139	8.065	6.560	63730	51701
	2	0.884	0.892	0.0198	0.0205	7.902	6.638	63231	52931
	5	0.852	0.882	0.0209	0.0225	8.548	7.066	71477	57333
	10	0.827	0.854	0.0267	0.0285	8.437	7.044	71640	57826
	15	0.788	0.817	0.0274	0.0279	8.793	7.417	76891	63004
100	1	0.675	0.680	0.0725	0.0453	13.199	10.790	125027	102505
	2	0.726	0.675	0.0545	0.0627	13.460	11.466	129579	110551
	5	0.582	0.540	0.0501	0.0791	13.872	12.365	135176	120639
	10	0.582	0.551	0.0606	0.0938	14.151	13.114	138645	128585
	15	0.512	0.515	0.0950	0.0987	14.296	13.556	140397	133262

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

V. CONCLUSION

An effective intrusion detection technique is proposed in this paper. The proposed approach uses least degree for-K algorithm. Intrusion-Detection Systems aims at detecting attacks against computer systems and networks, in general, attacks against information systems. IDS can be viewed as a guard system that automatically detects malicious activities within a host or network. As security is greatest issue in MANET, the paper can act as a source for the people working towards MANET.

REFERENCES

[1] Marti, Sergio, Thomas J. Giuli, Kevin Lai, and Mary Baker. "Mitigating routing misbehavior in mobile ad hoc networks." In Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255-265. ACM, 2000.
[2] Liu, Kejun, Jing Deng, Pramod K. Varshney, and Kashyap Balakrishnan. "An acknowledgment-based approach for the detection of routing misbehavior in MANETs." Mobile Computing, IEEE Transactions on 6, no. 5 (2007): 536-550.
[3] Sheltami, Tarek, Anas Al-Roubaiey, Elhadi Shakshuki, and Ashraf Mahmoud. "Video transmission enhancement in presence of misbehaving nodes in MANETs." Multimedia systems 15, no. 5 (2009): 273- 282.
[4] E. M. Shakshuki , N. Kang and T. R. Sheltami "EAACK—A secure intrusion detection system for MANETs", IEEE Trans. Ind. Electron., vol. 60, no. 3, pp.1089 -1098 2013.
[5] D. Dong, X. Liao, Y. Liu, C. Shen and X. Wang, "Edge Self-Monitoring for Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems," vol. 22, no. 3, March 2011, pp. 514-527.
[6] Khalil, S. Bagchi and N. B. Shroff, "SLAM: Sleep-Wake Aware Local Monitoring in Sensor Networks," Proc. 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2007 (DSN 2007), 565-574.
[7] T. Hoang Hai and E-N. Huh, " Optimal Selection and Activation of Intrusion Detection Agents for Wireless Sensor Networks," Proc. Future Generation Communication and Networking (FGCN 2007), vol.1, no., pp.350-355, 6-8 Dec. 2007.
[8] S. M. Fitaci, K. Jaffres-Runser and C. Comaniciu," On modeling energy security trade-offs for distributed monitoring in wireless ad hoc networks," Proc. Military Communications Conference, 2008. MILCOM 2008. IEEE, vol., no., pp.1-7, 16-19 Nov. 2008.
[9] N. Tsikoudis, A. Papadogiannakis and E. P. Markatos, "LEoNIDS: a Low-latency and Energy-efficient Network-level Intrusion Detection System," IEEE Transactions on Emerging Topics in Computing, Vol. PP, no. 99, 2014.
[10] Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks" In proceeding of the 1st ACM workshop on Security of ad hoc and sensor networks, pp.135-147, October 2003.
[11] C. Tseng, P. Balasubramanyam, C. Ko, R. Limsprasittiporn, J. Rowe, and K. Levitt. A specificationbased intrusion detection system for AO DV. In Proceedings of the 1st ACM workshop on Security of adhoc and sensor networks, pages 125-134, October 2003.