RESEARCH ARTICLE OPEN ACCESS

PERFORMANCE STUDY OF INTRUSION DETECTION TECHNIQUES IN MOBILE AD HOC NETWORKS

R.M.Chamundeeswari , Asst.Professor[1],
Department of Computer Applications,
Asan Memorial College of Arts & Science, Chennai.

Dr.P.Sumathi , Asst. Professor[2]
PG & Research Department ofComputerScience
Government Arts College, Coimbatore-18.

Abstract:

The mobile ad hoc network is an infrastructure less system of mobility appliance connected by wireless. The system protection violate cannot be prohibited using access and information flow control. This violate may be outcome system software and hardware failures interrelate system organizational actions or disappointment of the system verification module. The required for generate the existing methods into more difficult is in addition rising, because it result into fresh and other useful resolution. Intrusion detection is a significant part in the detection system abuse in many cases in current research works. An intrusion detection system is the capability to sense intruders and abuser actions in the system in a competent and sensible fashion. An Intruder that collaborate a mobile node in MANET eliminates the communication between the nodes. By distribution fake routing information, provided that false link status information, and plentiful other nodes with superfluous routing traffic information. The dependency and decentralized of MANET facilitate a challenger to enlarge innovative type of attacks that are measured to demolish the cooperative algorithms used in ad hoc networks. MANET is mostly susceptible to several kinds of attacks like inactive eavesdropping, dynamic impersonation, and denial of services. An Intruder that collaborate a mobile node in MANET obliterate the communication between the nodes by dissemination fake routing information. If inaccurate link state information, and abundant other nodes with superfluous routing traffic information. Therefore, successful implementation of MANET based on user's poise in its security. The security research in MANET has paying attention on key managing, routing protocol and intrusion detection techniques. Assessment on intrusion detection and supportive layer in MANET endow with resolution to extend their real world applications. In this paper, aspire to revision the various intrusion detections and prevention systems that were anticipated for Mobile Ad hoc Networks (MANETs). And then compare the latest techniques Intrusion Detection dependent on their architecture and data gathering techniques

1. INTRODUCTION

. The mobile nodes animatedly self structured into random topology networks devoid of a fixed infrastructure. The design of dynamic routing protocols with high-quality performance and a smaller amount overhead is main demand of mobile ah hoc networks. In particular, intrusion detection and response ability is extremely significant, as many real ad hoc networks. It determination be organize in aggressive environments in which genuine nodes can be captured and used by adversaries. There are two methods of to detecting the intrusion such as

- Misuse based intrusion detection
- Anomaly based intrusion detection.

The misuse detection also called as knowledge-based detection and anomaly based intrusion detection also called as behavior-based

detection. Fig 1.represent the intrusion detection structures of mobile ad hoc network system.

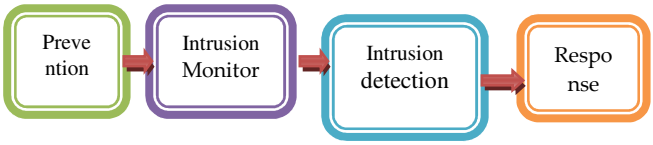

Fig 1.Architecture of IDS

The Misuse intrusion detection refers to the detection of intrusions by accurately crucial they further on of time and watching for their incidence. There is a

misuse constituent in the majority intrusion detection systems as statistical techniques unaided are not sufficient to detect all types of intrusions. Since statistical techniques alone are not adequate to detect all types of intrusions.

Anomaly detection is the detection of items, actions or annotations which do not be conventional to a predictable pattern or other items in a dataset. Typically the irregular items determination decode to some variety of difficulty such as bank fraud, a structural defect, checkup problems or finding errors in content. It stands against anomaly detection technique which utilizes the reverse technique of misuse intrusion detection. The anomaly detection is take first step to defining usual system behavior and than defining at all other behavior as irregular.

The aspiration suitable data dissemination approach is an essential in mobile ad hoc networks (MANET) owing to the repeated topology changes.

The Supportive communication has conventional incredible attention for mobile ad hoc network networks. The obtainable mechanism on supportive infrastructure is paying attention on link level corporeal layer issues. Accordingly, the impacts of supportive infrastructure on network level upper layer issues, such as topology control, map-reading and network capacity are largely disregarded.

The author used to some topology control related protocol to develop the topology manage scheme and then to improve the network capability in MANETs. By in cooperation behavior in intellect both upper layer systems capacity and physical layer compassionate communications. The physical layer sympathetic infrastructures have significant impacts on the network ability. The intended topology organize scheme can considerably improve the network capacity in MANETs with supportive infrastructure.

This paper is organized as follows: Section II discusses the classification of intrusion detection of mobile ad hoc network. Section III shows the analysis of recent techniques in active intrusion detection based techniques through disseminated and supportive layer in mobile ad hoc networks. Section IV describes the literature review in tabulation form by comparing the complete intrusion detection and topology control and data dissemination methods. Section V terminates the paper, solution areas of future research to expand their real world applications. Section VI discusses the future direction of these systems.

2. CLASSIFICATION OF INTRUSION DETECTION IN MANET COMMUNICATION

The most of the surviving protocols, applications and services for Mobile Ad Hoc Networks (MANETs) suppose a cooperative and responsive network environment and do not provide security. Consequently, the intrusion detection systems (IDSs), serve as the next line of protection for information systems, are essential for MANETs with elevated security requirements.

Intrusion Detection Techniques

i) Active Intrusion Detection
ii) Passive Intrusion Detection
iii) Network Intrusion Detection
iv) Host Intrusion Detection

The intrusion detection system can be separated into many ways. The major methods are active and passive intrusion detection, Network Intrusion detection systems (NIDS) and host Intrusion detection systems (HIDS)

An **Active Intrusion detection** system is as well described as Intrusion Detection and Prevention System. This system is configured to repeatedly block supposed attacks devoid of any interference required by an operator. This system has the gain of offering real time remedial action in response to an attack.

The **Passive Intrusion detection** is a system to facilitate configured to only monitor and evaluate network traffic activity and alerts an operator to probable vulnerabilities and attacks. A passive intrusion detection system is not competent of performing any defensive or remedial functions on its own.

The **Network Intrusion Detection** Systems frequently consists of a network sensor with a Network Interface Card operating in dissolute mode and a divide management interface. The intrusion detection system is located beside a network sector or boundary and monitors all traffic on those sectors.

The **Host Intrusion Detection** Systems and software relevance mediator installed on workstations which are to be monitored. The mediator monitors the operating system and writes data to log records and activate alarms. A host Intrusion detection systems can only observes the creature workstations on which the mediators are installed and it cannot supervise the total network. Host based IDS systems are used to observe any intrusion attempts on grave servers.

The Topology control is a method used in dispersed computing to modify the underlying network in regulate to reduce the cost of distributed algorithms unless ran over the fresh resulting graphs. Topology control is a crucial technique in distributed algorithm. The major aspire of topology control in this field is to save energy, reduce invasion between nodes and expand lifetime of the network system.

The Topology controls are dividing to main problems such as topology structure, in accuse of the

initial reduction and topology preservation. In accuse of the preservation of the abridged topology so individuality like connectivity and exposure are preserved.

Once the preliminary topology is set up, particularly when the position of the nodes is haphazard, the proprietor has no control over intend of the system. For example, some areas may be extremely substantial showing an elevated number of superfluous nodes. In which determination enlarge the number of significance collisions and Determination offer numerous copies of the similar information from likewise positioned nodes. Nevertheless, the proprietor has control over a number of restrictions of the system: transmission control of the nodes, situation of the nodes (active or sleeping), function of the nodes (Cluster head, gateway, regular), etc. By adapting these parameters, the topology of the system can revolutionize.

The leading the similar time a topology is abridged and the system starts serving its reason, the elected nodes create expenditure energy. The optimal abridged topology stops being it at the initial next of filled activity. After a few times being active, some nodes Determination establish to run out of energy. Particularly in wireless sensor networks with multi hoping, it is a fact that nodes that are nearer to the sink expend higher amounts of power that those beyond away owing to packet forwarding. The network must renovate the decrease network occasionally in organize to conserve connectivity, exposure, density and some other metric that the appliance requires.

3. VARIOUS TECHINIQUES OF ACTIVE INTRUSION DETECTION IN MOBILE AD HOC NETWORKS

3.1 IDS Methods for Manet

This paper is a survey of variety of Intrusion Detection System for MANETS dependent on their structural design and data gathering methods. Intrusion detection is the progression of monitoring the events up in a computer organization or system, and to evaluates them for cryptogram of feasible incidents. In which are contravention or impending threats of contravention of computer security policies, suitable use policies, or usual security practices. An intrusion prevention system (IPS) is software that has all the ability of an intrusion detection scheme and can also effort to end probable incidents. Surveillance of different research papers for intrusion detection and through dissemination supportive layer with topology control mechanisms is detailed below:

The reasonably susceptible to malicious system attacks security is a more important issue than infrastructure dependent wireless networks. In MANETs, it is complicated to identify malicious nodes as the topology of the system animatedly changes. As described a novel [1] anomaly detection method dependent on a dynamic learning progression that tolerates the preparation data to be restructured at exacting time intervals. The active learning progression engage calculating the projection reserve dependent on multidimensional data using weighted coefficients and a disregard the curve. The dynamic anomaly detection method is not reliable in intellect the intrusion and not succeeds in scrutinize the dissimilar kinds of attacks.

Sink mobility has concerned much explore benefit in Wireless Sensor Networks (WSNs), As demonstrated
a moving approach for the mobile sink [3] which avoid tracking or sense on it by rival during its data collection stage around the sensor field. The moving approach aspired to choosing a route for mobile sink node, which minimizes the total number of message communication from all static sensor nodes to the mobile sink node and thereby falling the opportunity of being sense by the adversaries. The Moving approach is not resolute on the fixed node and the range of the entire networks is not flexible on the use pattern.

In mobile ad hoc networks, here are lots of applications in which mobile users distribute information. Nevertheless, both of these conservative works unspecified an exacting mobility model and did not completely examine the authority of the mobility on the predictable system. As demonstrated to quantify the influences of mobility on data availability [4] and expansion are not done in concrete protocol. They unspecified neither exact appliance nor precise procedure but they optional and enumerate numerous metrics that affect data availability.

There are many intrusion detection methods have been used and strongly interrelated to routing protocols, such as Watchdog and Path rater and Route guard. The watchdog/path raters are also called intrusion detection. Route guards are also called response. [7] Watchdog inhabits in every node and is dependent on overhearing. Nevertheless, if the node that is eavesdropping and exposure itself is malicious, then it can cause grave collision on system performance. The flaw of Watchdog and establish the intrusion detection method called Ex Watchdog. This system is its capability to determine malicious nodes

which can separation the network by incorrectly exposure other nodes as mischievous and then proceed to defend the network.

Cognitive radio network dependent on IEEE wireless regional area network and illustrate some of the security threats alongside it. The CRN to rapidly sense whether they are being attacked, an uncomplicated yet effectual IDS is then accessible. [8] As demonstrated the non-parametric cumulative sum (cusum) as the alter point detection algorithm to find out the irregular behavior owing to attacks. The IDS adopt an anomaly detection scheme and it profiles the CRN system limit through a knowledge phase. So, it is also capable to detect novel types of attacks.

The leader election is the incidence of egotistical nodes for intrusion detection in mobile ad hoc networks (MANETs). There are two main complication in attained this goal. Primary, devoid of motivation for serving others, a node might perform inconsiderately by lying about its residual resources [9] and circumvent being elected. Second, electing an optimal compilation of leaders to reduce the generally resource expenditure may acquire an excessive recital overhead, if such a selection requires flooding the system. They are used in two potential appliance settings, namely, Cluster Dependent Leader Election (CDLE) and Cluster Independent Leader Election (CILE).

The Alert aggregation is a significant associate task of intrusion detection. The goal is to identify and to cluster dissimilar alerts formed by small level intrusion detection systems, firewalls. As demonstrated new technique [10] for on line alert aggregation which is dependent on an active, probabilistic representation of the modern attack situation. Essentially, it can be regarded as a data tributary version of an utmost likelihood scheme for the opinion of the model parameters. As well, Meta alerts are marked with a delay of classically only a few seconds subsequent to scrutinizes the first alert belonging to an innovative attack illustration.

As represented the idleness management of varied wireless sensor networks exploit multipath routing to respond user queries in the occurrence of undependable and malicious nodes. They devise the exchange as an optimization [11] problem for animatedly formative the best redundancy stage to relate to multipath routing for intrusion tolerance. So that the query reaction is achievement likelihood is maximized as prolonging the functional lifetime. They developed the novel likelihood representation to examine the greatest redundancy stage in stipulations of path redundancy. They are relevant the scrutiny results get hold of to intend of an active redundancy management algorithm. To classify and be appropriate the best design parameter situation at runtime in reply to location changes, to exploit the HWSN lifetime.

The black hole attack on a MANET refers to an attack by a malicious node, which compulsorily obtain the route from a source to a destination by the distortion of progression number and hop count of the routing communication. The selective black hole is a node that can electively and alternately execute a black hole attack or achieve as a usual node. As they demonstrated numerous [13] IDS nodes are position in MANETs in order to sense and avoid discriminating black hole attacks. The intrusion detection nodes must be set in inhale mode in arranges to execute the so-called ABM (Anti-Black hole Mechanism). They utility, which is mainly used to approximation an apprehensive value of a node according to the irregular dissimilarity between the routing communications transmitted from the node.

The Mobile ad hoc networks is extremely susceptible to attacks owing to the open average, animatedly varying network topology, supportive algorithms, and lack of federal monitoring and executive point. The conventional way of defensive networks with firewalls and encryption software is no longer enough and effectual for individuals features. A dispersed intrusion detection [15] scheme dependent on timed automata is specified. A cluster dependent detection method is offered, where occasionally a node is designated as the observe node for a cluster. These observe nodes can not only construct restricted intrusion detection assessment, but as well considerately take fraction in global intrusion detection.

The unique system for data caching provisions the queries that are submitted by requesting nodes in particular nodes, called query directories (QDs). They uses these queries to situate the data (reply) that are hoard in the nodes that demand them, called caching nodes (CNs). The Smart server update mechanism become accustomed the progression of caching a data item and updating it by the server to its prettiness and its data renew rate at the server [22]. The property of cache assignment strategy and cache replication is not up to the recital. Utilizations are derivative in order to decide the gains of employing our system in the MANET.

3.2 Multimodal Detection Techniques

The multimodal biometric equipment offer possible resolution for permanent user to tool verification in elevated security mobile ad hoc networks (MANETs). The distributed shared verification and intrusion detection with data synthesis in such MANETs. The Multimodal biometrics is installing to work with enhanced intrusion detection systems to ease the inadequacy of uni modal biometric systems. Because both devices in the system has dimension [16] and assessment limitations, more than solitary device requirements to be elected and annotations can be compound to increase observation accurateness by using Dempster–Shafer theory for data fusion. The structure chooses whether user verification is required and which biosensors must be elected, based on the safety posture. The choices are complete in an entirely dispersed manner by all verification device and IIDS.

The Multimodal Biometric technology substitutes a significant role in giving security between users to tool authentications. They concentrated on the Intrusion Detection and verification with data fusion in MANET. To conquer the responsibility in unimodal biometric systems, [17] Multimodal biometrics is lay down out to effort with Intrusion Detection Systems. All devices have scope and assessment boundaries, much procedure to be chosen and with the help of Dempster-Shafter theory for data fusion surveillance accuracy gets augmented. Dependent on the safety posture, system terminate which biosensor (IDS) to pick and whether user verification is indispensable. By all verification device and Intrusion Detection System the choice are complete in a fully dispersed manner.

3.3 MANET-Topology Control Protocol

MANETs are extremely susceptible to attacks due to the open intermediate, animatedly changing network topology and require of federal monitoring point. The different attacks alongside mobile nodes are flooding, black hole, warm hole, packet reducing and Byzantine attack etc. It is significant to explore fresh structural design and system to defend the wireless system and mobile computing application. [19] There are two techniques to analyze: misuse detection and anomaly detection. Misuse discovery is not effectual against unidentified attacks and consequently, irregularity detection method is used. In this method, the review data is composed from every mobile node subsequent to fake the attack and evaluated with the usual behavior of the scheme. They implementing two feature variety methods namely, markov blanket detection and genetic algorithm. In genetic algorithm, bayesian network is assembled over the composed features and vigor function is intended.

The Routing troubles have developed into extremely demanding as of the attractiveness of mobile devices. The targets power aware routing when system topologies and data traffic may modify rapidly in a random way. The distributed algorithm is a realization to exploit the least residual energy of all the nodes for every multicast, where no inclusive information is unspecified to be competently maintained at all nodes. The Maximum-Residual Multicast Protocol dependent on the self-sufficient alternative of intermediary nodes establish that the resultant tree is loop-free. And hypothetically the main optimal is the maximization of least residual energy [24]. The multisource maximum-residual multicast troubles and a variety of sources are not measured alongside.

The broadcasting technique is an appropriate for an extensive range of vehicular circumstances. Which only utilize limited information obtained via periodic beacon messages, hold acknowledgments of the [25] dispersed transmitted messages. Every vehicle chooses whether it go to a connected dominating set (CDS). The algorithm resolves broadcast at road traffic circle devoid of any required to even distinguish intersections. It is essentially flexible to dissimilar mobility regimes, devoid of the required to classify network or medium speeds.

Inferring the routing topology and linkage recital from a node to a set of extra nodes is a significant constituent in network monitoring and function design. The wide ranging structure for manipulative topology deduction algorithms [26] based on preservative metrics. The topology inference algorithms are achieving the better estimation accuracy. They probable that the possibility of precise topology inference of algorithms congregate to one exponentially fast in the number of inquisitive packets. An innovative sequential topology inference algorithm is to considerably reduce the inquisitive overhead and can competently handle node dynamics.

.The multiuser multiple input and multiple output (MIMO) networks, beneficiary deciphers numerous simultaneous signals using successive interference cancellation (SIC). The multiuser successive interference cancellation (MUSIC) is a structure that covetously forms and stimulates sub [28] topologies in an approach that discrimination. They

victorious SIC deciphering with an elevated probability. They provided together a centralized and a dispersed version of structure.

The MANET are regularly self-assured emphasize device with imperfect capabilities, competently manage sanctuary is vital to reduce the performance degradation and resource utilization. The MANET based on cooperative communication current important challenges to security concern in addition to concern of network recital and organization.

The Security is a significant problem in mobile ad hoc networks (MANETs). Nevertheless, security systems have important impacts on throughput. That is for the reason that 1) they required some transparency and use some network resources, thus reduce throughput accordingly; 2) The security and throughput disjointedly in manipulative a MANET, which can not accomplish an on the whole optimization of network recital.

The intrusion detection is a major problem in heterogeneous networks consisting of nodes with dissimilar non correlated protection assets. The game theoretical analysis based on to obtain the probable behaviors of normal attackers, [38] the least monitor source constraint, and the optimal approach of the protector. They offered guidelines for IDS intend and exploitation. They also how the game theoretical structures that can be functional to configure the intrusion detection plan in sensible scenarios via folder learning.

The cross-layer interaction between TCP and routing protocols in the IEEE 802.11 ad hoc network. They demonstrated the two complementary systems, that is, the TCP fractional window increment (Few) method [39] and the Route failure notification using Bulk loss Trigger (ROBUST) strategy. The TCP Few system is a defensive resolution used to diminish the congestion determined wireless link defeat. The ROBUST strategy is a curative resolution that facilitates on-demand routing protocols to contain overreactions stimulate by the violent TCP behavior.

One by one to get used to the time varying environment of wireless channels, a variety of channel adaptive method have been projected to utilize intrinsic spatial diversity in wireless ad hoc networks. In that way, to hunt for a theoretical foundation for humanizing spatial diversity expand, they prepare the [40] assortment of the next hop relay as a chronological decision difficulty and obtain a common. “Optimal Stopping Relaying (OSR)” structure for scheming such spatial-diversity schemes. They assuming Rayleigh fading channels, it implements an OSR approach to optimize information efficiency in a protocol hoard consisting of Greedy Perimeter Stateless Routing (GPSR) and IEEE 802.11 MAC protocols. The analysis only based of the algorithm for a particular node.

4.PARAMETRIC EVALUATION ON INTRUSION TECHNIQUES IN MANET

The existing Enhanced Adaptive Acknowledgment the utility of such exposure schemes all mostly based on the acknowledgment packets. These methods to accept a digital signature is named Enhanced AACK (EAACK).The possibilities of implement hybrid cryptography system to additionally to reduce the network overhead caused by digital signature. And as well as the possibilities of implement a key swap mechanism to eradicate the condition of pre distributed keys.

The Anti-Black whole Mechanism utility, which is mainly used to approximate a distrustful value of a node according to the irregular difference between the routing messages transmitted from the node. This method does not hold on the any key distribution and then authentication methods.

The Smart server updates mechanism reliability system is server dependent in which control method are executed to become accustomed the route of caching a data item. It modernizes it by the server to its attractiveness and its data update speed at the server. The main draw backs of the does not contain grasp effects of cache placement strategies and cache replication on performance.

The distributed cache invalidation mechanism is a pull dependent algorithm that implements adaptive time to live, associated, and perfecting, and gave near well-built consistency ability. The main disadvantages of the system more complicated TTL algorithms to reinstate the consecutively average function and does not execute the entire replica allocation.

The dynamic K edge connected topology control algorithm repeatedly verify the proper value of k for every local graph dependent on limited information as ensuring the essential connectivity ratio of the entire network. This method does not concentrate the acknowledgement based authentication in cross layer communication system.

Methods/Techniques	Parameters												
	Packet delivery ratio	End to End delay	Energy efficiency	Computational cost	Routing overhead	Packet delivery delay	Throughput	False Positive rate	Hit ratio	Execution Time	Percentage of IDS	Packet Loss rate	True positive rate
Adaptive Response Mechanism	Y					Y					Y		
Enhanced Adaptive Acknowledgment	Y				Y								
Watchdog And Path Rater					Y		Y						
Secure Leader Election Model			Y								Y		
Alert Aggregation	Y						Y				Y		
Redundancy Management		Y				Y		Y					Y
Classification Algorithms	Y		Y										
Anti-Black Hole Mechanism					Y						Y		
Multimodal Biometric IDS			Y				Y						Y
Cluster Dependent Detection	Y				Y						Y		
Dempster–Shafer				Y							Y		
Intrusion Detection With Data Fusion	Y					Y			Y				
Distributed Authentication And Intrusion Detection			Y		Y								
GA Based Feature Selection								Y					Y
Connected Dominating Set				Y		Y							
Topology Deduction Algorithms	Y												
K Edge Connected Topology Control Algorithms		Y									Y		
Multiuser Successive Interference Cancellation				Y									
Connectivity Dependent Topology Control	Y	Y		Y									
Game Theoretical		Y				Y						Y	
Fractional Window Increment						Y	Y						
Greedy Perimeter Stateless Routing	Y	Y					Y						

Parametrics on intrusion detection methods Note: Y-yes

The game theoretical is based on to acquire the possible behaviors of common attackers, the smallest amount monitor resource constraint, and the best possible approach of the protector. This method only verdict the only some type of IDS attacks must be implemented.

The multiuser successive interference cancellation a structure that acquisitively to forms and stimulate sub topologies. In a system that positive discrimination victorious SIC decipher with an elevated probability. Its also make certain that the number of elected sub topologies is reserved minute. The main problem of the MIMO network is the joint problem of stream control and link scheduling.

The cluster dependent and detection scheme is used periodically a node is designated as the observe node for a cluster. This observes nodes can not only make limited intrusion detection resolution, but does not cooperatively take part in global intrusion detection.

An Alert aggregation is dependent on a vigorous, probabilistic illustration of the contemporary attack circumstances. Alert aggregation is a significant sub assignment of intrusion detection. The objective is to discover and to cluster dissimilar alerts formed by low level interruption detection systems. The main drawback of the system does not deliberate techniques for interestingness dependent communication approach for dispersed IDS.

5. CONCULSION

The existing techniques dynamic anomaly detection usually used to authenticate the exceptionality and the topology of the network thus avoid any malicious crowd from combination the network. A conclusion that IDS structural design that entail cross layer design using independent mobile representative dependent architecture. In which is dispersed and supportive can competently detect the irregularity and is additional appropriate for mobile ad hoc networks.

To overcome these scheduling decisions, focus is made on developing dispersed development resolution combine authentication and intrusion exposure for efficient scheduling of information in MANET. In the dispersed development resolution, the most appropriate biosensors are animatedly elected dependent on the recent security posture and energy states. The biometric scheme controls in verification mode that single match method to covenant with an efficient scheduling. All biometric scheme give way of binary option and each one device are used at each time slot with multiple sources.

To realize this, Joint authentication and topology control using layer dependent exposure method is developed in MANET. Layer dependent exposure method deals in faultless the channel information and to accomplish exactness. The Layer based exposure intrusion detection method combine the suppleness of anomaly detection with the accuracy. In demanding, enlarge the machine learning technique in order to attain competent and efficient intrusion detection.

REFERENCES

[1] Hidehisa Nakayama., Satoshi Kurosawa, Abbas Jamalipour., Yoshiaki Nemoto., and Nei Kato., "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks," IEEE Transactions On Vehicular Technology, Vol. 58, No. 5, June 2009

[2] Elizabeth M. Daly., and Mads Haahr, "Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANET," IEEE Transactions on Mobile Computing, Vol. 8, No. 5, May 2009

[3] Zhou Sha., Jia-Liang Lu., Xu Li., Min-You Wu., "An Anti-Detection Moving Strategy for Mobile Sink," IEEE Global Telecommunications Conference (GLOBECOM 2010)

[4] Takahiro Hara, "Quantifying Impact of Mobility on Data Availability in Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, Vol. 9, No. 2, FEBRUARY 2010

[5] Adnan Nadeem, Michael, Howarth, "An Intrusion Detection & Adaptive Response Mechanism for MANETs" Journal of Elsevier Sep 2013

[6] Elhadi, Shakshuki, Nan Kang, Tarek and Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs ", IEEE Transactions on Industrial Electronics, Vol. 60, No. 3, March 2013

[7] Nidal Nasser and Yunfeng Chen, "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks Communications", 2007. ICC '07. IEEE International Conference on 24-28 June 2007

[8] Zubair Md. Fadlullah, Hiroki Nishiyama, and Nei Kato, "Intrusion Detection System (IDS) for Combating Attacks against Cognitive Radio Networks Zubair Network", IEEE (Volume: 27, Issue: 3), May-June 2013

[9] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET", IEEE transactions on dependable and secure computing volume: 8, issue: 1 2011 , page(s): 89 - 103

[10] Alexander Hofmann, Bernhard Sick, Member, "On-Line Intrusion Alert Aggregation with Generative Data Stream Modeling", IEEE Transactions on Dependable and Secure Computing, (Volume: 8, Issue: 2), March-April 2011

[11] Hamid Al-Hamadi and Ing-Ray Chen, "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks", IEEE Transactions on Network and Service Management, Vol. 10, No. 2, June 2013

[12] Aikaterini Mitrokotsa, Christos Dimitrakakis "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection", journal of Elsevier, 2012

[13] Ming-Yang Su "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", journal of Elsevier, 2011

[14] Parasakthi and sanjeev kumar, "Distributed Combined Authentication and Intrusion Detection in High-Security Mobile Ad Hoc Networks to reduce the computation complexity", National Conference on Advances in Computer Science and Applications with International Journal of Computer Applications (NCACSA 2012)

[15] Yi Ping, Jiang Xinghao, Wu Yue & Liu Ning "Distributed intrusion detection for mobile ad hoc network", Journal of Systems Engineering and Electronics Vol. 19, No. 4, 2008

[16] T.Kumanan and Duraiswamy "Dynamic Intrusion Detection with Data Fusion and Aggregation in High-Security Mobile Ad Hoc Networks", International Journal of Computer Science and Information Technologies, Vol. 3 (2), 2012, 3743-3748

[17] Lakshmi Narayanan and Fidal Castro "High Security for MANET Using Authentication and Intrusion Detection with Data Fusion", International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 1 ISSN 2229-5518

I.

[18] Jeyashree, "Highly Secure Distributed Authentication and Intrusion Detection with Data Fusion in MANET", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013

[19] R.Nallusamy, K.Jayarajan, Dr.K.Duraiswamy, "Intrusion Detection in Mobile Ad Hoc Networks Using GA Based Feature Selection", Georgian Electronic Scientific Journal: Computer Science and Telecommunications 2009|No.5 (22)

[20] Tapan P. Gondaliya, Maninder Singh, "Intrusion detection System for Attack Prevention in Mobile Ad-hoc Network", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 4, April 2013

[21] Shengrong Bu., F. Richard Yu., Xiaoping P. Liu., and Helen Tang., "Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks," IEEE Transactions on Wireless Communications, Vol. 10, No. 9, September 2011

[22] Khaleel Mershad and Hassan Artail., "SSUM: Smart Server Update Mechanism for Maintaining Cache Consistency in Mobile Environments," IEEE Transactions on Mobile Computing, Vol. 9, No. 6, June 2010

[23] Kassem Fawaz., and Hassan Artail., "DCIM: Distributed Cache Invalidation Method for Maintaining Cache Consistency in Wireless Mobile Networks," IEEE Transactions on Mobile Computing, Vol. 12, No. 4, April 2013

[24] Pi-Cheng Hsiu. And Tei-Wei Kuo, "A Maximum-Residual Multicast Protocol for Large-Scale Mobile Ad Hoc Networks," IEEE Transactions on Mobile Computing, Vol. 8, No. 11, November 2009

[25] Francisco Javier Ros, Pedro Miguel Ruiz and Ivan Stojmenovic, "Acknowledgment-Based Broadcast Protocol for Reliable and Efficient Data Dissemination in Vehicular Ad Hoc Networks", IEEE Transactions on Mobile Computing, Vol. 11, No. 1, January 2012

[26] Jian Ni, Haiyong Xie, Sekhar Tatikonda, and Yang Richard Yang, "Efficient and Dynamic Routing Topology Inference from End-to-End Measurements", IEEE/ACM transactions on networking, vol. 18, no. 1, February 2010

[27] Hiroki Nishiyama, Thuan Ngo, Nirwan Ansari, and Nei Kato, "On Minimizing the Impact of Mobility on Topology Control in Mobile Ad Hoc Networks", IEEE Transactions on Wireless Communications, Vol. 11, No. 3, March 2012

[28] Ece Gelal, Jianxia Ning, Konstantinos Pelechrinis, Tae-SukKim, Ioannis Broustis, Srikanth V. Krishnamurthy, and Bhaskar, "Topology Control for Effective Interference Cancellation in Multiuser MIMO Networks", IEEE/ACM Transactions on Networking, Vol. 21, No. 2, April 2013

[29] Quansheng Guan, Richard Yu, Shengming Jiang and Victor C. M. Leung, "Topology Control in Mobile Ad Hoc Networks with Cooperative Communications", IEEE Transaction on Wireless Communications, (Volume: 19, Issue: 2), April 2012

[30] Asha and Muniraj, "Network Connectivity based Topology Control for Mobile Ad Hoc Networks", International Journal of Computer Applications (0975 – 8887) Volume 56– No.2, October 2012

[31] Nasrin Shirali, "Topology control in the mobile ad hoc networks in order to intensify energy conservation", Journal of Elsevier Volume 37, Issue 24, 15 December 2013, Pages 10107–10122

[32] Asha and muniraj "Energy Efficient Topology Control Approach for Mobile Ad hoc Networks", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013

[33] Bharathi and saranya, "High Throughput Analysis Using Topological Control & Authentication Scheme in MANET", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 3, March 2013

[34] Quansheng Guan., F. Richard Yu., Shengming Jiang., and Victor C. M. Leung, "Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks with Cooperative Communications," IEEE Transactions on Vehicular Technology, Vol. 61, No. 6, July 2012

[35] Zhenzhen Ye and Alhussein A. Abouzeid, "Optimal Stochastic Location Updates in Mobile Ad Hoc Networks," IEEE Transactions on Mobile Computing, Vol. 10, No. 5, May 2011

[36] Jun-Won Ho., Wright, M.; Das, S.K., "Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis," IEEE, INFOCOM 2009

[37] Claire Le Goues., ThanhVu Nguyen., Stephanie Forrest., and Westley Weimer., "GenProg: A Generic Method for Automatic Software Repair," IEEE Transactions on Software Engineering, Vol. 38, No. 1, January/February 2012

[38] Lin Chen and Jean Leneutre "A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks", IEEE Transactions on Information Forensics and Security, Vol. 4, No. 2, June 2009

[39] Kitae Nahm, Ahmed Helmy, and Jay Kuo, Cross-Layer Interaction of TCP and Ad Hoc Routing Protocols in Multi hop IEEE 802.11 Networks", IEEE Transactions on Mobile Computing, Vol. 7, No. 4, April 2008

[40] Jing Ai, Alhussein A. Abouzeid and Zhenzhen Ye, "Cross-layer Optimal Decision Policies for Spatial Diversity Forwarding in Wireless Ad Hoc Networks", IEEE Transaction on wireless communication, Volume: 7 , Issue: 8 ,2008