ANALYTICAL SURVEY OF ACTIVE INTRUSION DETECTION TECHNIQUES IN MOBILE AD HOC NETWORKS

R.M.Chamundeeswari[1], P Sumathi[2]

[1]*Assistant Professor, Department Of Computer Application, Asan Memorial College of Arts & Science, Chennai*
[2]*Assistant Professor, PG and Research Department of Computer Science, Govt Arts College, Coimbatore*

Abstract

The mobile ad hoc network (MANET) is an infrastructure less system, comprises of mobile devices connected by wireless medium. MANET data communication undergoes various violation and prohibition issues by its mobile nodes, due to different access and information flow requirement across the network. In addition intermittent connectivity of wireless network and mobile device failures cause security lapses in the MANET communication, further leads to intruder's generating multiple attacks.. Intrusion detection gets more significant in current MANET security research works.

Furthermore due the open forum of MANET may change the system topology by suspecting attacks like inactive eavesdropping, dynamic impersonation and denial of services. To avoid all the problems created by an intruder, a successful MANET is implemented based on its security. The security research in MANET has been paying attention on key managing, routing protocol and intrusion detection techniques. The rating on intrusion detection and supportive layer in MANET has provided with a resolution to extend it to the real world applications. The active intrusion detection system aims to revise the various intrusion detections and prevention systems predicted for Mobile Ad hoc Networks (MANETs) and also compare the latest techniques of Intrusion Detection dependent on their architecture and data gathering techniques.

Keywords: *MANET, Intrusion Detection –AID, HIDS, NIDS, Topology, Attacks*

----------***----------

1. INTRODUCTION

Mobile ad hoc networks (MANETs) consist of collection of movable nodes, which move freely in the network. The mobile nodes change their structure and form a random topology networks as it deprived of a fixed infrastructure. The design of dynamic routing protocols with high-quality performance and a smaller amount of overhead is the main demand of mobile ah hoc networks. The Intrusion detection, which has been effectively used in wired networks to identify attacks, can offer a second line of defense. In particular, intrusion detection and response ability is extremely significant, as many real ad hoc networks. The system determines to be organized 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 as behavior-based detection. Fig 1.represent the intrusion detection structures of mobile ad hoc network system The Misuse intrusion detection refers to the detection of intrusions which are accurately crucial and further on time by watching for the incidence.

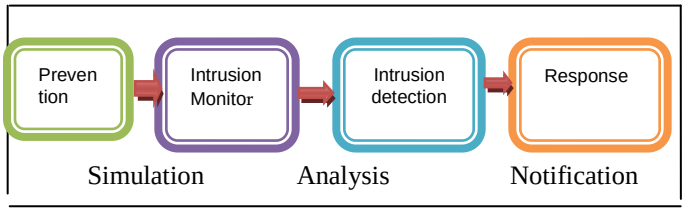

Fig 1 Architecture of IDS

If there is a misuse of a component, the majority. The statistical techniques alone are not adequate to detect all types of intrusions.

Anomaly detection is the detection of items, actions or annotations which are based on a predictable pattern or other items in a dataset.. It stands against anomaly detection technique which utilizes the reverse technique of misuse intrusion detection. The anomaly detection takes first step defining usual system behavior than defining all other behavior as irregular.

The aspiration suitable data dissemination approach is essential in mobile ad hoc networks (MANET) due to the repeated topology changes. There are two main methods which affect the data dissemination.

- Dynamic topology control,
- Resource constraint topology control

The Supportive communication has been remarkable attention for mobile ad hoc network networks. The available mechanism on supportive infrastructure is paying attention on link level corporeal layer issues. Accordingly, the impacts of the supportive infrastructure on network level upper layer issues, such as topology control, map-reading and network capacity are ignored. Fig 2.Represent the intrusion detection methods in agent based intruder in MANET Communication

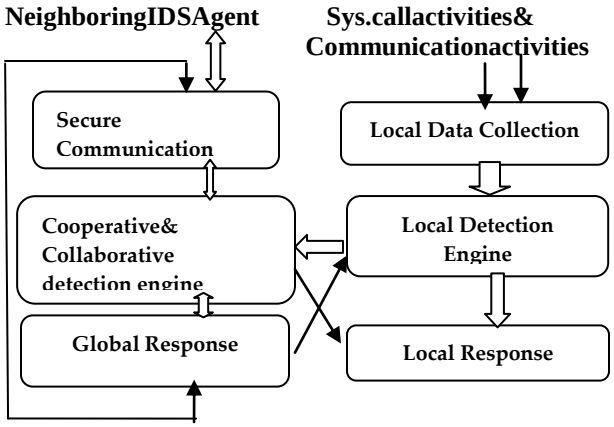

Fig2 IDS Agent Model

The author used some topology control related protocol to develop the topology and manage the scheme to improve the network capability in MANETs. By uncooperative behavior in intellect of both upper layer systems capacity and physical layer, the communications are compensated. The planned 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 IN INTRUSION DETECTION MANET COMMUNICATION

Most of the surviving protocols, applications and services for Mobile Ad Hoc Networks (MANETs) are supposed to be in cooperative and responsive network environment and will not provide security. Consequently, the intrusion detection systems (IDSs), serve as the next line of protection for information systems and are essential for MANETs with elevated security requirements.

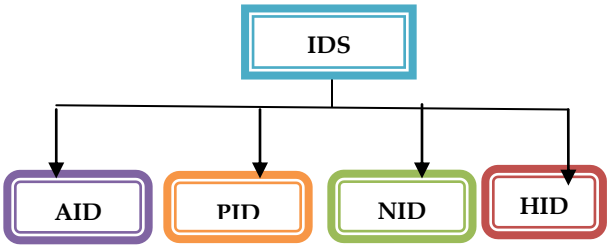

Fig 2 Classification of Intrusion detection system in MANET

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

An Active Intrusion detection system (**AID**) is as well described as Intrusion Detection and Prevention System. This system is configured to repeatedly block if the attacks devoid of any interference required by an operator.

The Passive Intrusion detection (**PID**) is a system to ease the configuration to only monitor and evaluate network traffic activity and alert an operator to check for probable vulnerabilities and attacks. A passive intrusion detection system doesn't have any ability of performing defensive or remedial functions on its own.
The Network Intrusion Detection(**NID**) Systems frequently consists of a network sensor with a Network Interface Card operating in dissolute mode and a divided 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 (**HID**) 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.

The Topology control is a method used in dispersed computing to modify the underlying network in regulating to reduce the cost of distributed algorithms unless there are no fresh resulting graphs.

The Topology controls are divided into main problems such as topology structure, in charge of the initial reduction and topology preservation, in charge of the preservation of the abridged topology, so the 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. 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. Leading. The optimal abridged topology stops being at the initial next of filled activity. After a few times being active, some nodes determine to run out

of energy. Particularly in wireless sensor networks with multi hoping, it is a fact the nodes that are nearer to the sink expend higher amounts of power that those beyond away due to packet forwarding.

3. ANALYSIS OF RECENT TECHNIQUES IN ACTIVE INTRUSION DETECTION IN MOBILE AD HOC NETWORKS

3.1 Various Intrusion Detection Methods in MANET

As described in the paper [1], the anomaly – detection scheme is based on a dynamic learning process that allows the training data to be updated at particular time intervals. As mentioned the MANET is an open medium and the network will be vulnerable to malicious attacks, so it is vital to expand efficient intrusion detection method to defend MANET from attacks. As represented and executed a fresh intrusion detection [6] method Enhanced Adaptive Acknowledgment (EAACK) particularly intended for MANETs. EAACK recognized as elevated malicious behavior exposure rates in assured conditions as it does not really influence the network performances.

A distributed intrusion detection [15] scheme is based on finish state machine. A cluster dependent detection method is offered, where occasionally a node is elected as the monitor node for a cluster.

The different attacks alongside mobile nodes are flooding, black hole, warm hole, packet reducing and Byzantine attack etc. which is important to search new architecture and mechanisms to protect the wireless networks. There are many intrusion detection methods which have been used and are strongly related to routing protocols, such as Watchdog and Pathrater and Routeguard. The watchdog is called intrusion detection and Routeguards/pathraters are called as response. [7] Watchdog inhabits in every node and is based on overhearing. Nevertheless, if the node that is eavesdropping and reporting itself is malicious, then it can cause serious impact on system performance.

Intrusion detection is used as a successive line of protection in Mobile Ad-hoc Networks. To carry out the protection they evaluate five supervised [12] categorization algorithms for intrusion exposures method. As they measure their performance on a dataset, which consist of different traffic conditions and mobility model for multiple attacks.

The selective black hole is a node that can electively and alternately execute a black hole attack or perform as a normal node. As they demonstrated, numerous [13] IDS nodes are deployed in MANETs in order to sense and avoid discriminating black hole attacks. Sink mobility has captivated much research interest in Wireless Sensor Networks (WSNs), because as demonstrated in moving approach for the mobile sink [3], which avoid tracking or sensing on it by adversaries during its data collection stage around the sensor field. There are lots of applications in Mobile Ad Hoc Networks in which mobile users distribute information. Nevertheless, each of these standard works guessed a particular mobility model and did not completely examine the authority of the mobility on the proposed system. The main aim is to quantify the influences of mobility on data availability [4] and expansions are not done in concrete protocol.

An intrusion detection and [5] adaptive reply mechanism for MANETs that senses a variety of attacks and offers an efficient reply with low network degradation. They considered the deficiencies of a fixed response to an intrusion and overcome the deficiencies with a flexible response scheme that depends on the measured confidence in the attack.

Insider attacks are one of the active attacks occurred in Ad-hoc network. An intrusion detection system will be developed for detection and isolation of attacks [20] and mac layer applications will be used for detecting malicious activities and will focus on the finding of attack sequences in the network. The Cognitive radio network to rapidly sense whether they are being attacked, a simple yet effective IDS is then presented. [8] The demonstrated non-parametric cumulative sum (cusum) as the change point detection algorithm to find out the irregular behavior due to attacks. The leader election is to balance the resource consumption among all nodes and extend the lifetime of a MANET and nodes with more remaining resources should be elected as the leaders. However, 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 remaining resources [9] and avoid being elected. 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 online alert aggregation which is dependent on a dynamic, probabilistic model of the current attack situation.

As represented in the social system analysis metrics that may be used to hold a new and practical [2] forwarding solution to provide competent message delivery in detached delay tolerant MANETs.

3.2 Multimodal Detection Techniques in MANET

The Multimodal is position to work with Intrusion Detection Systems (IDS) to assuage the shortcomings of unimodal [14] systems. The scheme chooses whether user verification is necessary based on the security posture. The decisions are made in a fully distributed manner by each verification device and IDS.

This technology is used to ease the inadequacy of uni modal systems. Since each device in the network has measurement [16]

and estimation limitations, more than one device needs to be elected and observation can be fused to increase observation accuracy by using Dempster–Shafer theory for data fusion.

All devices have dimensions and estimation limitation, many devices to be chosen and with the help of Dempster-Shafter theory for data fusion surveillance accuracy gets increased[17]. Based on the safety posture, system terminates which biosensor (IDS) to pick and whether user authentication is essential.

The Continuous user-to-device authentication is a demanding task in high security mobile AdHoc networks (MANETs). They are distributed combined authentication and intrusion discovery with data fusion [18] in such MANETs. To obtain the optimal scheme of combining continuous user authentication and IDSs in a distributed manner, they formulate the problem as a partially observable [21] Markov decision process (POMDP) multi-armed bandit problem. They present structural results method to solve the problem for a large network with a variety of nodes.

The consistency scheme is server-based in which control mechanisms are implemented to adapt the process of caching a data item and updating it by the server to its popularity and its data update rate at the server [22]. Distributed cache invalidation mechanism is a pull-based algorithm [23] that implements adaptive time to live (TTL), piggybacking, and prefetching, and provides near strong consistency capabilities.

The stochastic sequential decision framework [35] to analyze the problem under a Markovian mobility model, the location update decision problem is modeled as a Markov Decision Process (MDP). Then, given a separable cost structure, they show that the location update decisions of NU and LSU can be independently carried out without loss of optimality, i.e., a separation property.

The attacks which compromise the sensor nodes are dangerous because they allow the attacker to leverage the [36] compromise of a few nodes to exert control over much of the network.

GenProg uses an extended form of genetic programming to evolve a program variant that retains required functionality but is not susceptible to a given defect, using existing test suites to encode both the defect and required [37] functionality.

The game theoretical analysis derives the expected behaviors of rational attackers [38], the minimum monitor resource requirement, and the optimal strategy of the defenders. The guidelines for IDS design and deployment are provided.

3.3 Topology Control Protocols for MANET

The topology control has received much concentration in motionless sensor networks by efficiently reducing energy consumption, reducing interference, and limitation end-to-end delay, the transience of mobile nodes in Mobile Ad hoc Networks. The K edge connected topology control algorithms [27] are mainly used for the dynamic key methods. The multiuser successive interference cancellation (MUSIC) is a framework that greedly forms and stimulates sub [28] topologies in a way that favor successful SIC decoding with a high probability. The cooperative communications are [29] focused on link-level physical layer issues. The Capacity-Optimized Cooperative (COCO) topology control scheme is to improve the network capacity in MANETs by jointly considering both upper layer network capacity and physical layer cooperative communications.

The Network Connectivity based Topology Control (NCTC) to make [30] the correct the balance between interference and energy in order to improve the network lifetime of networks. The weighted and learning automata [31] dependent algorithm used to exaggerate energy preservation in a mobile ad hoc network.

The Energy Efficient Topology Control [32] Approach is developed to attain both network connectivity and energy consumption. While considering the spam attack in MANET with cooperative [33] communication results low throughput in network. So the proposed Secure Adaptive Distributed Topology Control Algorithm aims at topology control and performs secure self-organization in four phases i.e., Antinode Detection, Cluster Formation, Key Distribution and Key Renewal, to protect against malicious node attacks.

Security systems have important impacts on throughput. The topology control methods [34] are used to get better throughput by together manipulating upper layer security system and physical layer system. It's interrelated to channel circumstances and relay assortment for cooperative communications.

Routing problems have become highly challenging because of the popularity of mobile devices. A transient multicast tree is established on demand and derived based on the autonomous decisions of intermediate nodes. They proved that the derived tree is loop-free and theoretically optimal in the maximization of minimum residual energy [24].

The general framework for designing topology inference algorithms [26] based on additive metrics is used. The framework can flexibly fuse information from multiple measurements to achieve better estimation accuracy. The broadcasting algorithm suitable for a wide range of vehicular scenarios, which only employs local information acquired via periodic beacon messages, containing acknowledgments of the [25] circulated broadcast messages.

As represented the redundancy management of heterogeneous wireless sensor networks use multipath routing to respond user queries in the presence of undependable and malicious nodes. They devise the exchange as an optimization [11] problem for dynamically determining the best redundancy stage to relate to multipath routing for intrusion tolerance so that the query

reaction success probability is maximized while prolonging the functional lifetime.

4. ANALYSIS OF PEFORMANCE PARAMETERS ON WSN INTRUSION DETECTION METHODS

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

The Anti-Black whole Mechanism utility, which is mainly used to estimate an apprehensive value of a node according to the abnormal dissimilarity between the routing messages transmitted from the node. This method does not hold any key distribution and authentication methods.

The Smart server update is server-based in which control mechanisms are implemented to adapt the process of caching a data item and updating it by the server to its popularity and its data update rate at the server. The main drawback is it does not contain grasping effects of cache placement strategies and cache replication on performance.

The distributed cache invalidation mechanism is a pull-based algorithm that implements adaptive time to live (TTL), piggybacking, and prefetching, and provides near strong consistency capabilities. The main disadvantages of the system is when TTL algorithms are more complicated to reinstate the consecutively average function and does not execute the entire replica allocation.

The multiuser successive interference cancellation (MUSIC) is a framework that greedly forms and stimulates sub [28] topologies in a way that favor successful SIC decoding with a high probability

The cluster dependent and detection scheme is used when periodically a node is designated as the observe node for a cluster. This observing 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.

	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**
Anomaly Detection Scheme	**Y**	✓					**Y**				**Y**		
Disconnected Delay-Tolerant		**Y**					**Y**						
Anti-DetectionTechnique	**Y**			**Y**				**Y**					
Influences Of Mobility On Data Availability	**Y**			**Y**							**Y**		
Attack Prevention	**Y**			**Y**									
(POMDP)				**Y**						**Y**			
Smart Server Update Mechanism						**Y**			**Y**				
Distributed Cache Invalidation Method	**Y**								**Y**				
Maximum-Residual Multicast Protocol	**Y**			**Y**									
Cooperative Communications						**Y**							
Stochastic Sequential Decision				**Y**	**Y**								**Y**
Predetermined Sensor Locality	**Y**		**Y**							**Y**			**Y**

Fig : parametrics on intrusion deteion methods of WSN Y-refers to the usage of corresponding parameter in its method

5. CONCULSIONS

As the use of MANET has enlarged the security in MANETs, it has also developed into more significant. Chronological event explores that prevention only means cryptography and authentication, but they are not as much as necessary. Hence the IDS is fetching into the consideration.

The discussion about 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. After scrutinizing the architectures of IDS for MANETs they came to conclusion that IDS structural design that entail cross layer design using independent mobile representative dependent on architecture. In which the dispersed and supportive competently detect the irregularity and additionally it is appropriate for mobile ad hoc networks.

SCOPE OF FUTURE ENHANCEMENT

To accomplish the dynamic anomaly detection is to unconstraint the feature, and also some other nearest neighboring techniques. It preserves the dependent mechanism, where it introduced to examine the intrusions efficiently. The preserve dependent mechanism factor recognizes the similarity to usual classes and detects abnormal attacks. Nearest neighbor and preserve dependent mechanism frequently uses machine learning and ad-hoc network intrusion detection.

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 of the devices 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 with the faultless of the channel information and to accomplish exactness. The Layer based exposure intrusion detection method combine the suppleness of anomaly detection with the accuracy. In demand is to 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
[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