Intrusion Detection System for Security of Mobile Communication Using Watchdog and Pathrater

Anju R. Fule **Dr. S.S. Sherekar** **Prof. V.M. Thakare**

Abstract —**The information transferred between nodes is made secure by Intrusion detection system (IDS) using techniques watchdog and path rater. By eavesdropping on the transmission of the next hop, the watchdog finds the misbehaving nodes. A path rater helps to identify the routes that do not contain n those misbehaving nodes. The watchdog is implemented by maintaining a buffer of recently sent packets. Comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If a packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet.**

Key Words — **MANET, IDS, Watch Dog, Path rater**

I. INTRODUCTION

Mobile communication is spread all over the world. To developed high security in mobile communication and take action against attacks required prevention, detection and recovery. There is need to be provide security for secure communication by mobile. Intrusion detection system is used to detected the intrusion in the node. The basic function of IDS is to collected data, detection and response.

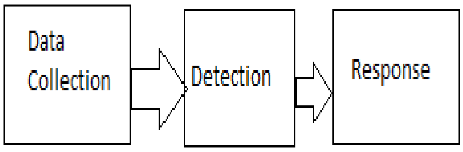

Fig. 1 Intrusion detection System

IDS having three techniques 1. Anomaly based IDS 2. Misuse based IDS 3. Specification based IDS.

1. Anomaly Detection:

Anomaly detection systems focus on normal behaviours, rather than attack behaviours. First these systems describe what constitutes a “normal” behaviour (usually established by automated training) and then flag as intrusion tries any activities that differ from this behaviour by a statistically significant amount.

2. Misuse Detection:

In misuse detection or signature based detection systems, the observed behaviour is compared with known attack patterns (signatures). Action patterns that may pose a security threat must be defined and stored to the system. Then, the misuse detection system tries to recognize any “bad” behaviour according to these patterns.

3. Specification Based:

Specification based detection systems are also based on deviations from normal behaviour in order to detect attacks, but they are based on manually defined specifications that describe what a correct operation is and monitor any behaviour with respect to these constraints.

II. BACKGROUND

Intrusion Detection is suggested as an approach to prevent unauthorized access to a system [1]. Most of the intrusion detection systems are not such dynamic to overwhelm misuses and anomalies. A system, program or person who tries to get unauthorized access to some system resources or who tries to break down system functionality is called an intruder [2]. Intrusion Detection Systems (IDS) try to detect the attempts to break down the system integrity and privacy, anomalies and unauthorized access to system resources [3]. IDS provide reports on system activity to help system administrators to understand abnormal situations [4]. Clifton and Gengo [5] considers that false alarms appear in the alert because normal operation with similar characteristics of the invasion occurs in a particular environment, and the alarms caused by these operations have a certain sequential pattern.

III. PREVIOUS WORKDONE

Nadiammai et al. [1] has proposed Effective approach toward Intrusion Detection System using data mining techniques. Data mining concept is integrated with IDS to identify the relevant, hidden data of interest for the user effectively and with less execution time. Four issues such as Classification of Data, High Level of Human Interaction, Lack of Labeled Data, and Effectiveness of Distributed Denial of Service Attack are being solved using the proposed algorithms like EDADT algorithm, Hybrid IDS model, Semi-Supervised Approach and Varying HOPERAA Algorithm respectively. Proposed algorithm has been tested using KDD Cup dataset. All the proposed algorithm shows better accuracy and reduced false alarm rate when compared with existing algorithm.

Cho et al. [2] has proposed Effect of Intrusion Detection on Reliability of Mission-Oriented Mobile Group Systems in Mobile Ad Hoc Networks. Analyze the effect of intrusion detection system (IDS) techniques on the reliability of a mission oriented group communication system consisting of mobile groups set out for mission execution in mobile adhoc networks. Unlike the common belief that IDS should be executed as often as possible to cope with insider attacks to prolong the system lifetime, discover that IDS should be executed at an optimal rate to maximize the mean time to failure of the system. Further, the optimal rate at which IDS is executed depends on the operational conditions, system failure definitions, attacker behaviors and IDS techniques used. Develop mathematical models based on Stochastic Petri nets to identify the optimal rate for IDS execution to maximize the mean time to failure of the system, when given a set of parameter values characterizing the operational conditions, and attacker behaviors.

Wang et al. [3] has proposed A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks. Recent advances in mean field game theory, propose a novel game theoretic approach with multiple players for security in MANETs. The mean field game theory provides a powerful mathematical tool for problems with a large number of players. The proposed scheme can enable an individual node in MANETs to make strategic security defence decisions without centralized administration. In addition, since security defence mechanisms consume precious system resources (e.g., energy), the proposed scheme considers not only the security requirement of MANETs but also the system resources. Moreover, each node in the proposed scheme only needs to know its own state information and the aggregate effect of the other nodes in the MANET. Therefore, the proposed scheme is a fully distributed scheme. Simulation results are presented to illustrate the effectiveness of the proposed scheme.

Dong Ma et al. [4] has proposed a Synergetic Pattern Matching Method Based-on DHT Structure for Intrusion Detection in Large scale Network. A warning by analyzing the behavior of the log, the contents of the relevant association, through the DHT (Distributed Hash Table) distributed architecture, the Collabarative matching, fusion, and ultimately determine the method of attack paths. First, by improving the classical Apriori algorithm, greatly improving the efficiency of the association. At the same time, through the behavior pattern matching algorithms to extract information about the behavior of the alert and the behavior sequence elements to match the template, and through the right path to finally determine the value of the threat of the network path. After the design of a DHT network, the distributed collaborative match the path used to find complex network attacks. Finally, the overall algorithm flow, proposed complete threat detection system architecture.

Tosun et al. [5] has proposed Policy Misuse Detection in communication networks with Hidden Markov Model. IDS provide a high level security between organizations while preventing misuses and intrusions in data communication through internet or any other network. Adherence to network usage policies is crucial since a system or network administrator needs to be informed whether the information is compromised, if the resources are appropriately used or if an attacker exploits a comprised service. Server flow authentication via protocol detection analyzes penetrations to a communication network. Generally, port numbers in the packet headers are used to detect the protocols. However, it is easy to re-map port numbers via proxies and changing the port number via compromised host services. Using port numbers may be misleading for a system administrator to understand the natural flow of communications through network. It is also difficult to understand the user behavior when the traffic is encrypted since there is only packet level information to be considered. Present a novel approach via Hidden Markov Models to detect user behavior in network traffic. Perform the detection process on timing measures of packets. The results are promising and obtained classification accuracies between %70 and %100.

IV. EXISTING METHODOLOGY

Proposed EDADT (Efficient Data Adapted Decision Tree) algorithm Framework: The hybrid PSO technique to identify the local and global best values for n number of iterations to obtain the optimal solution. The best solution is obtained by calculating the average value and by finding the exact efficient features from the given training data set. For each attribute select all unique values of a to find the unique values belong to the same class label. If n unique values belong to the same class label, split them into m intervals, and m must be less than n. If the unique values belong to different c class label, check whether the probability of the value belongs to same class. If it is found then change the class label of values with the class label of highest probability. Split the unique values as c interval then repeat checking of unique values in the class label for all values in the data set. Find out the normalized information gain for each attribute and decision node forms a best attribute with the highest normalized information gain. Sublists are generated using best attributes and those nodes forms the child nodes. These processes continue until the data set converges. Train the EDADT model.

V. ANYLASIS AND DISCUSSIONS

KDD Cup 99 data set has been used in this research of which 60% is treated as training data and 40% is considered as testing data. The proposed framework has been implemented in MatLab10 and Java using data mining techniques. Performance of four proposed methods such as,

_ Classification of network data using EDADT algorithm.
_ Proposed Hybrid IDS.
_ Performance of Semi-Supervised Approach for IDS and,
_ Mitigating DDoS attacks using Varying Clock Drift Mechanism.

Trained 5 Hidden Markov Models for each protocol. Used 25000 telnet, smtp, nntp, Domain records and 5000 login records. Two parameters: packet size and packet duration. First analyzed the training data. Used k-means clustering and divided each training set to 9 clusters. For 5 protocols, 9 ×5 = 45 clusters are selected. Separated each group of packets as small and large packets. The states of the model represent whether a packet is small or large. Used duration and packet size parameters to detect protocols. These parameters were failure to detect protocols exactly because some protocols dominate others in specific regions. Moreover, they can be transmitted for a long time interval overlapping with other protocols.

VI. PROPOSED METHODOLOGY

WATCHDOG AND PATHRATER

Watchdog and Path rater, to be added on top of the standard routing protocol in adhoc networks. The watchdog method detects misbehaving nodes. The watchdog finds the misbehaving nodes by eavesdropping on the transmission of the next hop. A path rater then helps to identify the routes that do not contain those misbehaving nodes. In DSR, the routing information is defined at the source node. This routing information is passed together with the message through intermediate nodes until it reaches the destination. Therefore, each middle node in the path should know who the next hop node is.

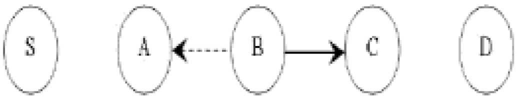

Fig.2 watchdog works: Although node B intends to transmit a packet to node C, node A could eavesdrop this transmission.

Assume that node S wants to send a packet to node D, and there exists a path from S to D through nodes A, B, and C. Consider now that A has already received a packet from S destined to D. The packet contains a message and routing information. When A forwards this packet to B. A also keeps a copy of the packet in its buffer. Then A listens to the transmission of B to make sure that B forwards to C. If the packet overheard from B (represented by a dashed line) matches that stored in the buffer, it means that B really forwards to the next hop (represented as a solid line).

It then removes the packet from the buffer. However, if there's no matched packet after a certain time, the watchdog increments the failures counter for node B. If this counter exceeds the threshold, A concludes that B is misbehaving and reports to the source node S. The watchdog is implemented by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If a packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node. The watchdog technique has disadvantages and advantages. DSR with the watchdog has the advantage that it can detect misbehavior at the forwarding level and not just the link level. Watchdog's disadvantages are that it might not detect a misbehaving node in the presence of Ambiguous collisions, Receiver collisions, Limited transmission power, false misbehavior, Collusion, and Partial dropping.

The ambiguous collision problem prevents A from overhearing transmissions from B. A packet collision can occur at A while it is listening for B to forward on a packet. A does not know if the collision was caused by B forwarding on a packet as it should or if B never forwarded the packet and the collision was caused by other nodes in A's neighborhood. Because of this uncertainty, A should not immediately accuse B of misbehaving, but should instead continue to watch B over a period of time. If A repeatedly fails to detect B forwarding on packets, then A can assume that B is misbehaving.

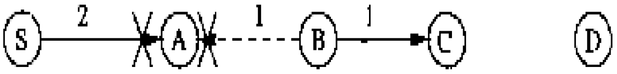

Fig 3. Ambiguous collision, Node A does not hear B forward packet 1 to C because B's transmission collides at A with packet 2 from the source S.

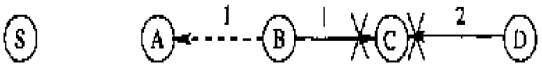

Fig 4. Receiver collision, Node A believes that B has forwarded packet 1 on to C, though C never received the packet due to a collision with packet 2.

In the receiver collision problem, node A can only tell whether B sends the packet to C, but it cannot tell if C receives it. If a collision occurs at C when B first forwards the packet, A only sees B forwarding the packet and assumes that C successfully receives it. Thus, B could skip retransmitting the packet. B could also purposefully cause the transmitted packet to collide at C by waiting until C is transmitting and then forwarding on the packet. In the first case, a node could be selfish and not want to waste power with retransmissions. In the latter case, the only reason B would have for taking the actions that it does is because it is malicious. B wastes battery power and CPU time, so it is altruistic.

An overloaded node would not engage in this behavior either, since it wastes badly needed CPU time and bandwidth. Thus, this second case should be a unusual happen.

The Watchdog mechanism: Every time a network entity (si,m, monitoring entity) needs to monitor the correct execution of a function implemented in a neighboring entity (sj,o, observed entity), it triggers a WD specific to that function(f). The WD stores the expected result er(f) in a temporary buffer in si,m and verifies if the observed result or(f) and er(f)match. If the monitored function is executed properly then the WD removes from the buffer the entry corresponding to the sj,o, er(f) couple and enters in an idle status, waiting for the next function to observe. On the other hand, if the function is not correctly executed or if the couple sj,o, er(f) remains in the buffer for more than a certain time out, a negative value to the observation rating factor ok is reported to the entry corresponding to sj,o in the RT and a new reputation value for that entity is calculated. It should be noticed that the term Expected result corresponds to the correct execution of the function monitored by the WD, which is substantially different from the final result of the execution of the function.

VII. Possible Outcomes And Result

MANETs in order to set up the route with reliability between transmission pair. This approach may cause a serious contention in information transfer between adjacent nodes and a considerable amount of control packets. The transfer of information between nodes is made secured by Intrusion detection system (IDS). IDS is to achieve the reliable and confidential transmission over MANET with techniques such as Watch Dog, Path rater.

Conclusion

This paper presents a Intrusion Detection System (IDS) to make a secured MANET by IDS which are proposed for adhoc mobile networks and also provide techniques of IDS. It has presented techniques such as Watchdog and Path rater for detecting the attacks in nodes. DSR with the watchdog has the advantage that it can detect misbehavior at the forwarding level and not just the link level.

References

[1] Jin Hee Cho , "Effect of Intrusion Detection on Reliability of Mission Oriented Mobile Ad Hoc Networks", IEEE Transactions on Reliability, Vol.59 No. 1 , p.p. 231-241, 2010.

[2] Yanwei wang, "A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks", IEEE Transactions, Vol.13 No. 3, p.p. 1616-1626, March 2014

[3] Zubir Md. Fadlullah, "Intrusion Detection System for combating Attack s Against Cognitive Radio Networks", IEEE Transaction, Vol No. 0890-8044, p.p.51-56 , 2013

[4] Dong Ma, "A Synergetic pattern matching based on DHT Structure for intrusion Detection in Large scale Network", Springer, Vol No. 1877-7058, p.p. 3511-3515 , 2011

[5] Umut Tosun, "Policy Misuse Detection in Communication Networks with Hidden Markov Models", Science Direct, Vol No.32, p.p. 947-952, 2014

Author's Profile

	Anju Fule Anju R. Fule has completed B.E. Degree in Padmabhooshan Vasantdada Patil Institute of Technology, Bavdhan, Pune, Maharashtra. She is persuing Masters Degree in Computer Science and Information Technology from P.G. Department of Computer Science and Engineering, S.G.B.A.U. Amravati.

	Dr. Swati Sherekar Dr. Swati Sherekar received the degree of M.Sc. and Ph.D in computer science from SGB Amravati University, Amravati. Presently working as Associate professor in the P. G. Department of Computer Science and Engg. and having 19 years of teaching experience. Her area of research is Network security, data security, Image Processing and completed her Ph.D. in multimedia authentication. Completed one MRP. Number of papers are on her credits at National & International level journals and conferences.

	Dr. Thakare sir Dr. Vilas M. Thakare is Professor and Head in Post Graduate department of Computer Science and engineering Faculty of Engineering & Technology, SGB Amravati university, Amravati. He is also working as a coordinator on UGC sponsored scheme of e-learning and m-learning specially designed for teaching and research. He is Ph.D. in Computer Science/Engineering and completed M.E. in year 1989 and graduated in 1984-85. He has exhibited meritorious performance in his studentship. He has more than 27 years of experience in teaching and research. Throughout his teaching career he has taught more than 50 subjects at various UG and PF level courses. He has done his PhD in area of robotics, AI and computer architecture. He has completed one UGC research project MRP. He has published more than 150 papers in international and national level Journals and also international Conferences and national level Conferences.