Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Intrusion Detection Techniques for Cooperation of Node in Mobile ad hoc network (MANET)

Mangalmoy Pradhan[1], Rakesh Kumar Singh[2]

[1,2]*IIMT COLLEGE OF ENGINEERING, Greater Noida*

Abstract—Since there is no infrastructure in mobile ad hoc networks, each node must rely on other nodes for cooperation in routing and forwarding packets to the destination. Intermediate nodes might agree to forward the packets but actually drop or modify them because they are misbehaving. The simulations in show that only a few misbehaving nodes can degrade the performance of the entire system. There are several proposed techniques and protocols to detect such misbehavior in order to avoid those nodes, and some schemes also propose punishment as well.
It is very difficult to design once-for-all intrusion detection techniques. Instead, an incremental enhancement strategy may be more feasible. A secure protocol should at least include mechanisms against known attack types. In addition, it should provide a scheme to easily add new security features in the future. Due to the importance of MANET routing protocols, we focus on the detection of attacks targeted at MANET routing protocols This include WatchDog and Pathrater approach. A watchdog identifies the misbehaving nodes by eavesdropping on the transmission of the next hop. A path rater then helps to find the routes that do not contain those 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.

Keywords—MANET, Watchdog, Path rater, DSR

I. INTRODUCTION

In adhoc networks do not rely on pre-existing infrastructure and this may be their most distinguishing attribute. Instead ad hoc networks are formed by individual nodes when they come to close proximity and need to communicate with each other. This implies that there is no need for stationary components such as routers, bridges and cables and of course central administration is not required. Due to the lack of stationary infrastructure, the participating nodes in the ad hoc network have to forward traffic on behalf of other nodes that are not in close proximity to the destination node. If they deny participating in the routing process, the connectivity between nodes may be lost and the network could be segmented. Therefore, the functionality of an ad hoc network heavily depends on the forwarding behavior of the participating nodes.
Ad hoc networks can be characterized as autonomous in the sense that most commonly they offer connectivity between the participating nodes and not connectivity to external LANs or internets. However in theory it is possible that some of the ad hoc nodes are multi-homed with connections in both the ad hoc network and one or more external networks. Nothing prevents these nodes from acting as gateways between these networks but is not a common element.
Another very important property [20] of ad hoc networks is their dynamic topology. Since the topology arbitrarily changes due to node mobility and changes of the surrounding environment, the utilized routing protocols have to be able to adapt to the dynamic topology. Traditional wired routing protocols like OSPF do not incorporate in their normal operation support for frequent network topology changes. Thus, the routing protocols that are currently utilized in adhoc environments have specifically been designed to handle node mobility and rapidly changing topologies. The devices that

are usually employed in the ad hoc networks have their own limitations. Since, the only hardware component that is required to connect a device in an ad hoc network is a wireless interface, PDAs and mobile telephones can be utilized. Furthermore, differences in the radio transmission ranges and reception equipment sensitivities may lead to unidirectional links which could complicate routing in the ad hoc networks. Apart from the communication differences between the nodes, ad hoc networks suffer from limited hardware resources like limited battery, constrained CPUs and small memory capacity.

Advantages of Mobile Ad-hoc Networks

There are several advantages [20] of using mobile ad hoc network.

- Setting up a wireless system is easy and fast and it eliminates the need for pulling out the cables through walls and ceilings.
- Network can be extended to places, which cannot be wired.
- Multiple paths increase reliability.
- Wireless network offers more flexibility and adapt easily to changes in the configuration of the network.

Limitations of Mobile Ad hoc Networks

There are certain constraints [16] found in MANET, described below:

Asymmetric links: Most of the wired networks rely on the symmetric links, which are always fixed. But this is not a case with ad-hoc networks as the nodes are mobile and constantly changing their position within network.

Routing Overhead: In wireless ad hoc networks, nodes often change their location within network. So, some out-of-date routes are generated in the routing table, which leads to unnecessary routing overhead.

Interference: This is the major problem with mobile ad-hoc networks as links come and go depending on the transmission characteristics, one transmission might interfere with another one and node might overhear transmissions of other nodes and can corrupt the total transmission.

Dynamic Topology: This is also the major problem with ad-hoc routing since the topology is not constant. The mobile node might move or medium characteristics might change. In ad-hoc networks, routing tables must somehow reflect these changes in topology and routing algorithms have to be adapted. For example in a fixed network routing table updating takes place for every 30sec. This updating frequency might be very low for ad-hoc networks.

II. SAMPLE INTRUSION DETECTION SYSTEMS FOR MANETS

Since the IDS for traditional wired systems are not well-suited to MANETs,many researchers have proposed several IDS especially for MANETs, which some of them will be reviewed in this section.

Distributed and Cooperative IDS

The model for an IDS agent is structured into six modules. The local data collection module collects real-time audit data, which includes system and user activities within its radio range. This collected data will be analyzed by the local detection engine module for evidence of anomalies. If an anomaly is detected with strong evidence, the IDS agent can determine independently that the system is under attack and initiate a response through the local response module (i.e., alerting the local user) or the global response module (i.e., deciding on an action), depending on the type of intrusion, the type of network protocols and applications, and the certainty of the evidence.

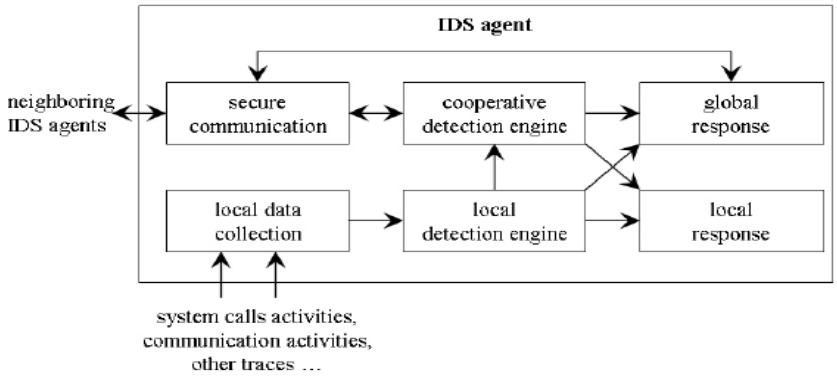

Figure 1: Model for an IDS Agent

If an anomaly is detected with weak or inconclusive evidence, the IDS agent can request the cooperation of neighboring IDS agents through a cooperative detection engine module, which communicates to other agents through a secure communication module.

Local Intrusion Detection System (LIDS)

Albers et al[15]. proposed a distributed and collaborative architecture of IDS by using mobile agents. A Local Intrusion Detection System (LIDS) is implemented on every node for local concern, which can be extended for global concern by cooperating with other LIDS.

Two types of data are exchanged among LIDS: security data (to obtain complementary information from collaborating nodes) and intrusion alerts (to inform others of locally detected intrusion). In order to analyze the possible intrusion, data must be obtained from what the LIDS detect, along with additional information from other nodes. Other LIDS might be run on different operating systems or use data from different activities such as system, application, or network activities; therefore, the format of this raw data might be different, which makes it hard for LIDS to analyze. However, such difficulties can be solved by using SNMP (Simple Network Management Protocol) data located in MIBs (Management Information Base) as an audit data source. Such a data source not only eliminates those difficulties, but also reduces the increase in using additional resources to collect audit data if an SNMP agent is already run on each node.

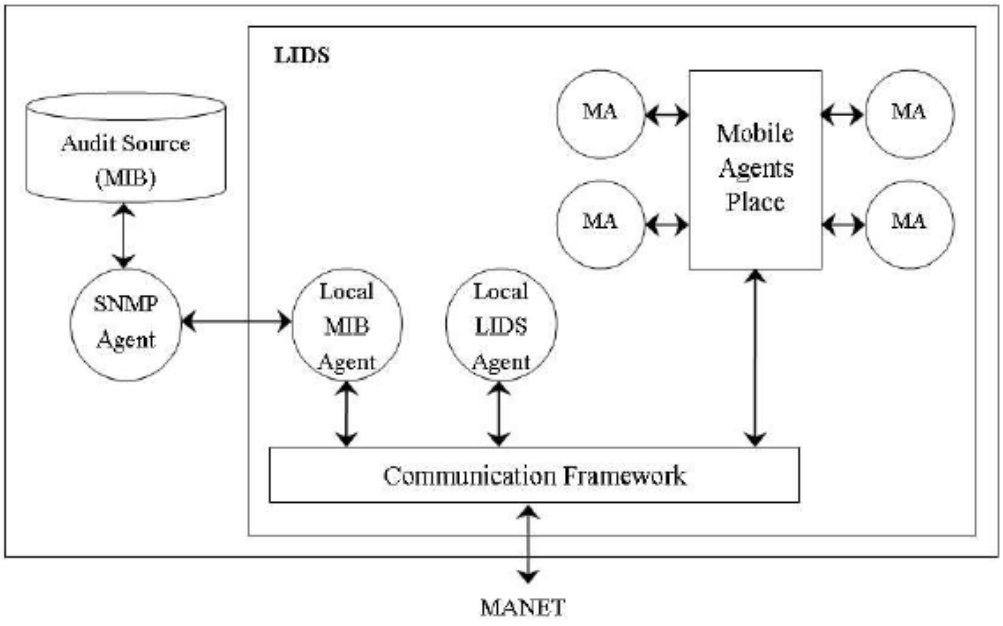

Figure 2: LIDS Architecture[15] in Mobile node

The LIDS architecture is shown in above Figure which consists of

- Communication Framework: To facilitate for both internal external communication with a LIDS.
- Local LIDS Agent: To be responsiblefor local intrusion detection and local response. Also, it reacts to intrusion alerts sent from other nodes to protect itself against this intrusion.
- Local MIB Agent: To provide a means of collecting MIB variables for either mobile agents or the Local LIDS Agent. Local MIB Agent acts as an interface with SNMP agent, if SNMP exists and runs on the node, or with a tailor-made agent developed specifically to allow updates and retrievals of the MIB variables used by intrusion detection,if none exists.
- Mobile Agents (MA): They are distributed from its LID to collect and process data on other nodes. The results from their evaluation are then either sent back to their LIDS or sent to another node for further investigation.
- Mobile Agents Place: To provide a security control to mobile agents.

Distributed Intrusion Detection System Using Multiple Sensors

Kachirski and Guha[20] proposed a multi-sensor intrusion detection system based on mobile agent technology. The system can be divided into three main modules, each of which represents a mobile agent with certain functionality: monitoring, decision-making or initiating a response. By separating functional tasks into categories and assigning each task to a differentagent, the workload is distributed which is suitable for the characteristics of MANETs. In addition, the hierarchical structure of agents is also developed in this intrusion detection system.

- Monitoring agent: Two functions are carried out at this class of agent: network monitoring and host monitoring. A host-based monitor agent hosting system-level sensors and user-activity sensors is run on every node to monitor within the node, while a monitor agent with a network monitoring sensor is run only on some selected nodes to monitor at packet-level to capture packets going through the network within its radio ranges.
- Action agent: Every node also hosts this action agent. Since every node hosts a host-based monitoring agent, it can determine if there is any suspicious or unusual activities on the host node based on anomaly detection. When there is strong evidence supporting the anomaly detected, this action agent can initiate a response, such as terminating the process or blocking a user from the network.

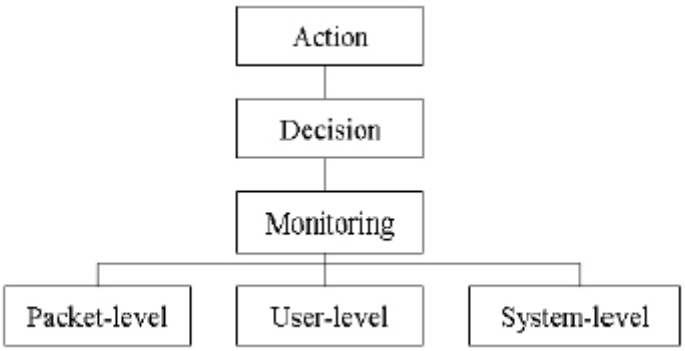

Figure 3 : Layered Mobile Agent Architecture proposed by Kachirski and Guha

- Decision agent: The decision agent is run only on certain nodes,mostly those nodes that run network monitoring agents. These nodes collect all packets within its radio range and analyze them to determine whether the network is under attack. Moreover, from the previous

paragraph, if the local detection agent cannot make a decision on its own due to insufficient evidence, its local detection agent reports to this decision agent in order to investigate further.

The network is logically divided into clusters with a single cluster head for each cluster. This cluster head will monitor the packets within the cluster and only packets whose originators are in the same cluster are captured and investigated. This means that the network monitoring agent (with network monitoring sensor) and the decision agent are run on the cluster head. In this mechanism, the decision agent performs the decision-making based on its own collected information from its network-monitoring sensor; thus, other nodes have no influence on its decision. This way, spoofing attacks and false accusations can be prevented.

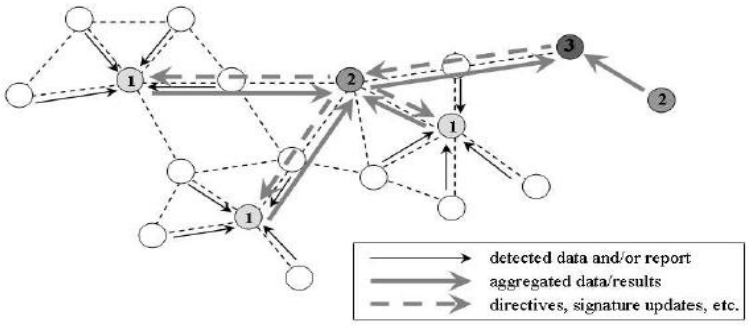

Figure 4 : Dynamic Intrusion Detection Hierarchy[25]

Cooperative Intrusion Detection System

A cluster-based cooperative intrusion detection system, similar to Kachirski and Guha's system , has been presented by **Huang and Lee[21]** . In this approach, an IDS is not only able to detect an intrusion, but also to identify the attack type and the attacker, whenever possible, through statistical anomaly detection. Various types of statistics (or features), are evaluated from a sampling period by capturing the basic view of network topology and routing operations, as well as traffic patterns and statistics, in the normal traffic. Hence, attacks could be identified if the statistics deviate from the pre-computed ones (anomaly detection).Statistics can be categorized into two categories, non traffic-related and traffic related. Non traffic-related statistics are calculated based on the mobility and the trace log files, which can be done separately on each node.

Several identification rules are pre-defined for known attacks by using relationships of the mentioned statistics. Once an anomaly is detected, the IDS will perform further investigation to determine the detailed information of the attack from a set of these identification rules. These rules enhance the system to identify the type of the attack and, in some cases, the attacking node. Some notations of statistics are presented as follows.

Let M represent the monitoring node and *m* represent the monitored node.

- #(*;m): the number of incoming packets on the monitored node m.
- #(*; [m]): the number of incoming packets of which the monitored node m is the destination.
- #(m; *): the number of outgoing packets from the monitored node m.
- #([m]; *): the number of outgoing packets of which the monitored node m is the source.
- #(m; n): the number of outgoing packets from m of which n is the next hop.
- #([s];M;m): the number of packets that are originated from s and transmitted from M to m.
- #([s]; [d]): the number of packets received on m which is originated from s and destined to d.
- #(*;m)(TY PE = RREQ): the number of incoming RREQ packets on m.

These statistics are computed over a long period *L*. Let *FEATUREL* represents the aggregated *FEATURE* over time *L*. Some identification rules are defined for well known attacks as follows.

- Unconditional Packet Dropping:This rule uses Forward Percentage (*FP*) over a period *L* to define the attack.

$$FPm = \frac{\text{Packet actually forwarded}}{\text{Packet to be forward}} = \frac{\#L(m;M) - \#L([m];M)}{\#L(M;m) - \#L(M;[m])}$$

If there are packets to be forwarded (denominator is not zero) and *FPm* = 0, the unconditional packet dropping attack is detected and the attacker is *m*.

- Random Packet Dropping: This rule also uses the same FP unconditional packet dropping. However,the threshold FP is defined as FP<1.
  If 0 < FPm < FP , m is defined an attacker using random packet dropping.
- Selective Packet Dropping: This rule uses Local Forward Percentage (LFP) for each source s

$$LFP_m^s = \frac{\text{packets from source } s \text{ actually forwarded}}{\text{packets from source } s \text{ to be forwarded}} = \frac{\#^L([s],m,M)}{\#^L([s],M,m) - \#^L([s],M,[m])}$$

If the denominator is not zero and *LFP* = 0, the attack is the unconditional packet dropping targeted at *s*. However, if *LFPsm*is less thanthe threshold (*LFP* < 1), the attack is detected as random packet dropping targeted at *s*.

- Blackhole: This rule uses Global Forward Percentage (GFP) and it must be computed on M locally because the rule relies on information available only on the node. Let N(M) denote M's 1-hop neighbors.

$$GFP_m^s = \frac{\text{packets to be forwarded}}{\text{packets from} N(M) \text{destined to other nodes than itself or another} N(M)} = \frac{\#^L(*,M) - \#^L(*,[M])}{\sum_{i \epsilon N(M)} \#^L(i,M) - \sum_{i,j \epsilon N(M)} \#^L(i,[j]) - \#^L(*,[M])}$$

If the denominator is not zero and *GFP* = 1, it means that the black- hole attack is detected and *M* is the attacker.

- Malicious Flooding *on* specific target :This rule uses *#L*([*m*]; [*d*]) for every destination d. If it is larger than the threshold the attack is Malicious Flooding. However, the attacker cannot be determined

Intrusion Detection Based on a Static Stationary Database

A distributed IDS has been proposed at **Mississippi State University[1]** in which each node on the network has an IDS agent running on it . The IDS agents on each node in the network work together via a cooperative intrusion detection algorithm to decide when and how the network is being attacked. The architecture is divided into parts: the mobile IDS agent, which resides on each node in

the network, and the stationary secure database, which contains global signatures of known misuse attacks and stores patterns of each user's normal activity in a non-hostile environment.

- Mobile IDS Agents Each node in the network will have an IDS agent running on it all the time. This agent is responsible for detecting intrusions based on local audit data and participating in cooperative algorithms with other IDS agents to decide if the network is being attacked. Each agent has five parts: a local audit trial, a local intrusion database (LID), a secure communication module, anomaly detection modules(ADMs), and misuse detection modules (MDMs).
- The LID is a local database that warehouses all information necessary for the IDS agent, such as the signature files of known attacks, the established patterns of users on the network, and the normal traffic flow of the network.The ADMs and MDMs communicate directly with the LID to determine if an intrusion is taking place.
- The secure communication module is necessary to enable an IDS agent to communicate with other IDS agents on other nodes. It will allow the MDMs and ADMs to use cooperative algorithms to detect intrusions. It may also be used to initiate a global response when an IDS agent or a group of IDS agents detects an intrusion. Data communicated via the secure communication module needs to be encrypted.

.

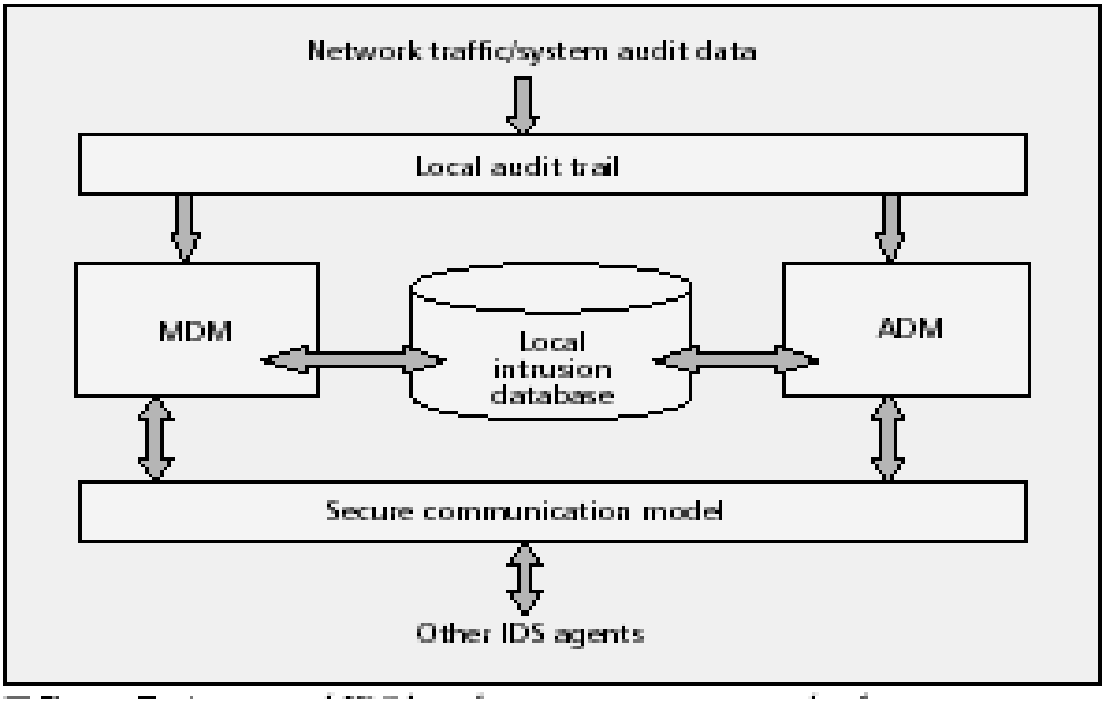

Figure 5: An IDS Based On Stationary Secure Database

- The ADMs are responsible for detecting a different type of anomaly. There can be from one to many ADMs on each mobile IDS agent,each working separately or cooperatively with other ADMs.
- The MDMs identify known patterns of attacks that are specified in the LID. Like the ADMs, if the audit data available locally is sufficient to determine if an intrusion is taking place, the proper response can be initiated. It is also possible for an MDM to use a cooperative algorithm to identify an intrusion.

III. RECENT WORK IN INTRUSION DETECTION TECHNIQUES FOR NODE COOPERATION IN MOBILE AD HOC NETWORKS (MANET)

Watchdog and Pathrater

Two techniques were proposed by **Marti, Giuli, and Baker[11],** watchdog and Path rater, to be added on top of the standard routing protocol in adhoc networks. The standard is Dynamic Source Routing protocol (DSR)

A watchdog identifies the misbehaving nodes by eavesdropping on the transmission of the next hop. A path rater then helps to find the routes that do not contain those 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 intermediate node in the path should know who the next hop node is. In addition, listening to the next hop's transmission is possible because of the characteristic of wireless networks - if node A is within range of node B, A can overhear Communication to and from B

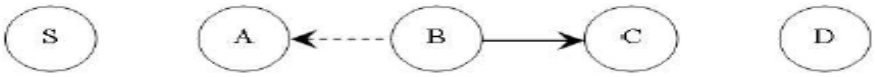

Figure 6 : How Watchdog works: Although node B intends to transmit a packet to node C, node A could overhear this transmission.

Reputation Based Schemes.

Reputation systems are used in many areas of electronic transactions, such as eBay and Amazon. Reputation mechanisms are applied to wireless mobile ad hoc network to address threats arising from uncooperative nodes. They rely on neighbor monitoring to dynamically assess the trustworthiness of neighbor nodes and excluding untrustworthy nodes.

Several reputation systems have been proposed to mitigate selfishness and stimulate cooperation in mobile ad hoc network, including:

- CONFIDANT
- CORE
- OCEAN

CONFIDANT

Buchegger and Boudec[4] present a reputation based protocol, called CONFIDANT, for making misbehavior unattractive . CONFIDANT stands for Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Network, it works as an extension to on demand routing protocols. CONFIDANT aims at detecting and isolating uncooperative nodes, thus making it unattractive to deny cooperation. Nodes rely on passive observation of all packets within a one-hop neighborhood. With CONFIDANT, each node has the following four components: a monitor, a trust manager, a reputation system and a path manager. These components interact with each other to provide and process protocol information.

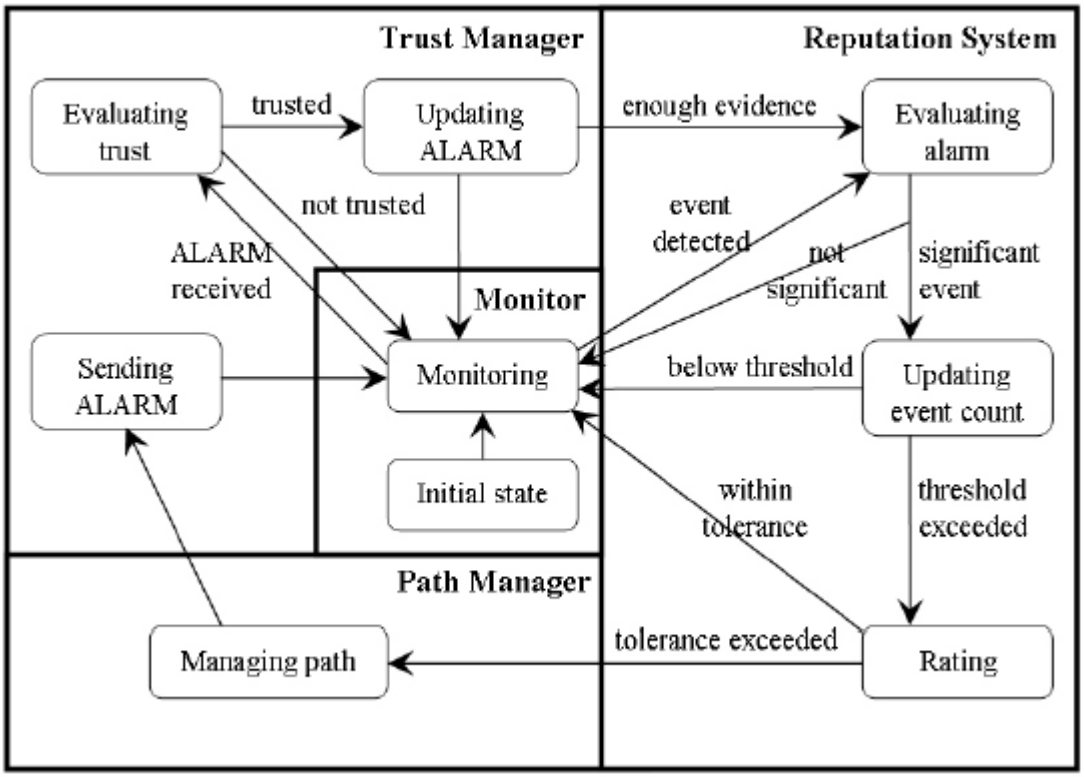

Figure 7:Components and State Diagram of CONFIDANT Protocol

- Monitor :The monitor is the equivalent of a "neighbor watch", where nodes locally monitor deviating behavior. A node can detect deviation and their rating. The rating is changed only when there is sufficient evidence of malicious by its neighbor on the source route by listening to the transmission of its neighbor.The monitor reports any suspicious events and any incoming ALARM messages to the trust manager.
- Trust Manager: The trust manager makes decisions about providing or accepting route information, accepting a node as part of a route, or taking part in a route originated by another node. It consists of the following components:

    - An alarm table containing information about received alarms.
    - A trust table managing trust levels for nodes to determine the trustworthiness of an alarm.
    - A friends list containing all the \friends" that the node may sends alarms to.

- Reputation System: The reputation system in this protocol manages a table consisting of entries for nodes and their rating. The rating is changed only when there is sufficient evidence of malicious behavior that is significant for a node and that has occurred a number of times exceeding a threshold to rule out coincidences. To avoid a centralized rating, local rating lists and/or black lists are maintained at each node and potentially exchanged with friends.
- Path Manager: The path manager performs the following functions: path re-ranking according to reputation of the nodes in the path; deletion of paths containing malicious nodes, action on receiving a request for a route from a malicious node (e.g. ignore, do not send any reply) and action on receiving request for a route containing a malicious node in the source route (e.g. ignore, alter the source).

Each node monitors the behavior of its neighbors. If a suspicious event is detected, the information is given to the reputation system. If the event is significant for the node, it is checked whether the event has occurred more often than a predefined threshold that is high enough to distinguish deliberate malicious behavior from simple coincidences such as collisions.

CORE

P. Michiardi etal[7]. proposed a mechanism called CORE (COllaborative REputation mechanism), to enforce node cooperation in mobile ad hoc network. It is a generic mechanism that can be integrated with any network function like packet forwarding, route discovery, network management and location management. CORE stimulates node cooperation by using a collaborative monitoring technique and a reputation mechanism. In this mechanism, reputation is a measure of someone's contribution to network operations. Members that have a good reputation can use the resources while members with a bad reputation, because they refused to cooperate, are gradually excluded from the community.

CORE defines three types of reputation:

- Subjective reputation is a reputation value which is locally calculated based on direct observation. For example, node A calculates the reputation of a neighbor node B at a given time for a particular function.
- Indirect reputation is second hand reputation information which is established by other nodes. For example, in CORE, node A will accept the indirect reputation of node B from node C. To eliminate an attack where a malicious node disseminates false negative reputation information, only positive reputation information is distributed in CORE.
- Functional reputation is related to a certain function, where each function is given a weight as to its importance. For example, data packet forwarding may be deemed to be more important than forwarding packets with route information, so data packet forwarding will be given greater weight in the in the reputation calculations.

OCEAN

S. Bansal et al[9]. proposed an Observation-based Cooperation Enforcement in Ad hoc Networks (OCEAN) .In contrast to CONFIDANT and CORE, OCEAN avoids indirect (secondhand) reputation information and uses only direct first-hand observations of other nodes behavior.A node makes routing decisions based solely on direct observations of its neighboring nodes interaction.

OCEAN has five components reside in each node to detect and mitigate misbehavior:

- Neighbor Watch observes the behavior of the neighbors of a node. It works the same way as watchdog .Whenever misbehavior is detected, Neighbor Watch reports to the RouteRanker, which maintains ratings of the neighbor nodes.
  .
- RouteRanker maintains a rating for each of its neighboring nodes. The rating is initialized to Neutral and is incremented and decremented based on observed events from the NeighborWatch component.

- Rank-Based Routing uses the information from NeighborWatch to make the decision of selection of routes. An additional field, called the avoid-list, is added to the DSR Route-Request Packet (RREQ) to avoid routes containing nodes in the faulty list.

- Malicious Traffic Rejection rejects traffic from nodes which is considered misbehaving. All traffic from a misbehaving node are rejected so that a node is not able to relay its own traffic under the guise of forwarding it on.

- Second Chance Mechanism allows nodes previously considered misbehaving to become useful again. A timeout approach is used where a misbehaving node is removed from the faulty list after a fixed period of inactivity .Even though the node is removed from the faulty list, its rating is not increased, so that it can quickly be added back to the faulty list if it continues the misbehavior.

OCEAN focuses on the robustness of packet forwarding: maintaining the overall packet throughput of mobile an ad hoc network with the existence of misbehaving nodes at the routing layer. OCEAN approach is to disallow any second-hand reputation exchanges. Routing decisions are made based solely on direct observations of neighboring nodes behavior. This eliminates most trust management complexity.
However, in contrast to the previous approaches above, OCEAN relies only on its own observation to avoid the new vulnerability of false accusation from second-hand reputation exchanges. Therefore, OCEAN can be considered as a stand-alone architecture.

IV. CONCLUSION

Intrusion detection techniques for cooperation of node in MANET which include WatchDog and Pathrater approach. It also present Reputation Based Schemes in which Reputation regarding every node is calculated and is circulate to every node in network. Reputation is defined as Someone's contribution to network operation.. In this, we have critically examined the existing systems and outlined their strength and shortcomings. We have opted an approach for our system in terms of mode of information propagation among nodes. The goal was to design a system incorporating the best traits of all existing systems without incurring extra routing overhead

REFERENCES

[1] S.Madhavi **"**Intrusion Detection in Mobile Adhoc Networks". In Proceedings of International Conference on Information Security and Assurance, vol 8, July2008, IEEE.
[2] Y.Xiao,X Shen, A Survey on Intrusion Detection in Mobile AdHoc Networks. In Proceedings of Wireless and Network Security, pp 176-190 June 2006.
[3] Sonja Buchegger and Jean-Yves Le Boudec, "Self-Policing Mobile Ad-Hoc Networks by Reputation Systems" IEEE Communication Magazine, vol. 43, No. 7, p. 101, 2005.
[4] S. Buchegger and J. L. Boudec. Performance Analysis of the CONFIDANT protocol: Cooperation of nodes | fairness in dynamic ad-hoc Networks. In Proceedings of IEEE/ACM Symposium on Mobile AdHoc Networking and Computing (MobiHoc), Lausanne, CH, June 2005.
[5] Anand Patwardhan, Anupam Joshi, Jim Parker, Michaela lorga; Secure Routing and Intrusion Detection in Adhoc Networks. In the Proceedings of the 3rd International Conference on Pervasive Computing and Communications(PerCom 2005), Kauai Island, Hawaii, July 2005.
[6] G. Vigna, S. Gwalani and K. Srinivasan, An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks, Proc. of 20th Annual Computer Security Applications Conference (ACSAC'04).
[7] P. Michiardi, R. Molva, Core: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks, Institut EurecomResearch Report RR-02-062 – December, 2004.
[8] S. Buchegger and J.-Y. Le Boudec: The effect of Rumor Spreading in Reputation Systems for Mobile ad-hoc Networks" Proc. WiOpt'03(Modeling and Optimization in Mobile Ad Hoc and Wireless Networks), (2004).
[9] Sorav Bansal and Mary Baker, "Observation based cooperation enforcement in ad hoc networks" Technical Report, Stanford University, arXiv:cs.NI/0307012 v2 6 Jul (2003).
[10] Sonja Buchegger, Cedric Tissieres, Jean-Yves Le Boudec, "A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Networks How Much Can Watchdogs Really Do?," Sixth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'04), pp. 102-111, (2003).

[11] S. Buchegger and J.-Y. Le Boudec, "The effect of rumor spreading in reputation systems for mobile ad-hoc networks" Proc. WiOpt'03(Modeling and Optimization in Mobile Ad Hoc and Wireless Networks), (2003).
[12] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt. A specification-based intrusion detection system for AODV. In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pages 125–134. ACMPress, 2003.
[13] Semih Dokurer, Y.M Erten.Performance Analysis of Black Hole Attack under Adhoc Network Proceedings of the 3rd ACM international Symposium on Mobile AdHoc Networking Computing Lausanne,Switzerland, June 09 - 11, 2002 MobiHoc '02
[14] Sonja Buchegger, Jochen Mundinger, Jean-Yves Le Boudec. Reputations System for Self Organized Network. IEEE Communications Magazine, pages 101–107, July 2002.
[15] Asad Amir Pirzada and Chris McDonald. Establishing trust in Adhoc Networks. In Proceedings of 27th Australasian Computer ScienceConference, The University of Otago, New Zealand. in Research and Practice in Information TechnologyVol. 26,August 2001.
[16] C. E. Perkins, "Ad hoc Networking", Addison-Wesley, 2001.
[17] Y. Zhang and W. Lee. Intrusion Detection in Wireless Ad Hoc Networks. In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000), August, 2000.
[18] Zheng Yan, Peng Zhang, Teemupekka Virtanen. Trust Evaluation Based Security Solution in Ad Hoc Networks Proceedings of MobiCom 2000, Sixth Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 6-11 Aug. 2000
[19] J. Broch, D. Johnson, and D. Maltz. The dynamic source routing protocol for mobile Adhoc networks. Internetdraft draft-ietf- manet-dsr-01.txt, December 1999.
[20] S. Corson, J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", Request For Comments(RFC) 2501, January 1999.
[21] C. Perkins, E. Royer and S. Das, "AODV routing", Internet Draft draftietf-manet-aodv-13.txt,Feb 1999
[22] L. Zhou, Z.J. Haas, "Securing Ad hoc Networks", IEEE, Networks Magazine,Vol. 13, no 6, November/December, 1999.
[23] J.Allen et al., State of Practice of Intrusion Detection Technologies, Tech Report CMU/SEI-99-TR-028, October 1998.
[24] Cannady, J and J.Harell ."A Comparative Study of Current Intrusion Detection Technologies". 4th Technology for information Security Conference, pp186-189
[25] K.Scarfone and P.Well Guide to Intrusion detection and prevention system.Technical report 800-94, NIST,1997

