ISSN No. 0976-5697

Volume 4, No. 6, May 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICAL

Available Online at www.ijarcs.info

Intrusion Detection for eliminating Security Issues in Wireless Mobile Ad Hoc Networks

P. R Ubhale*[1], A. M. Sahu[2]

Computer Science & Engg. , S.G.B.A.U.Amravati. G.H.Raisoni College of Engg. & Magt., Amravati (MH)India.

[1]panku_ubhale@yahoo.co.in, [2]amit.3696sahu@gmail.com

***Abstract*—** In this paper, we discuss security issues and their current solutions in the mobile ad hoc network. Ad hoc networks are a new wireless network for mobile hosts. As the need for innovative and efficient means of information exchange, wireless networks are increasingly being used to address these demands with limited costs to infrastructure requirements. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. While the routing aspects of mobile ad hoc networks (MANETs) are already well understood, the research activities about security in MANETs are still at their beginning. The military aspects and other security-sensitive operations are still using ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. The strength of its infrastructure (wireless nature) also becomes the point of its greatest vulnerability. Thus decreasing the confidence level of the system as it pertains to availability, reliability, data integrity and privacy concerns. Wireless networks indeed are an effective means of communication for a variety of platforms. Also MANETs pose a number of new security problems in addition to the problems of regular networks. In addition to the classical security threats we identified additional ways how nodes may attack security in an Ad hoc network. Finally we outline a security architecture that provides substantial security services for Ad hoc networks.

Due to the nature of the wireless media, ad-hoc wireless networks are vulnerable to various attacks. There are security protocols that prevent unauthorized nodes from accessing the network through authentication. Secrecy of information is provided through encryption. However these protocols cannot detect if any member of the network degrades the network performance due to misbehavior. Therefore an intrusion detection system (IDS) is required that monitors what is going on in the network, detects misbehavior or anomalies based on the monitored information and notifies other nodes in the network to take necessary steps such as to avoid or punish the misbehaving nodes.

***Keywords*—** MANET (Mobile Ad Hoc Network) SPREAD, Impersonation, Intrusion, IDS Agent, Ad Hoc, DSR

I. INTRODUCTION

In an ad hoc network, there is no fixed infrastructure such as base stations or mobile switching centres. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. Figure 1 shows such an example: initially, nodes A and D have a direct link between them. When D moves out of A's radio range, the link is broken. However, the network is still connected, because A can reach D through C, E, and F. For example, military units (e.g., soldiers, tanks, or planes), equipped with wireless communication devices, could form an ad hoc network when they roam in a battlefield. Ad hoc networks can also be used for emergency, law enforcement, and rescue missions. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms. Security is a critical issue in a mobile ad hoc network (MANET). As compared with an infrastructure or wired network, a MANET poses many new challenges in security. For example, wireless channel is more vulnerable to attacks such as passive eavesdropping, or active signal interference and jamming; the co-operative MANET protocols are more vulnerable to denial of service attacks; the lack of infrastructure and limited resources restrict the applicability of some conventional security solutions; and the un-predictable ad hoc mobility makes it more difficult to detect the malicious behaviour [1].

Figure 1: Topology change in ad hoc networks: nodes A, B, C, D, E, and F constitute an ad hoc network. The circle represents the radio range of node A. The network initially has the topology in (a). When node D moves out of the radio range of A, the network topology changes to the one in (b).

A. *Security attributes:*

Security is an important issue for ad hoc networks, especially for those security-sensitive applications. To secure an ad hoc network, we consider the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation.

- ***a.*** ***Availability*:** ensures the survivability of network services despite denial of service attacks.
- ***b.*** ***Authentication*:** enables a node to ensure the identity of the peer node it is communicating with.
- ***c.*** ***Non-repudiation*:** ensures that the origin of a message cannot deny having sent the message.
- ***d.*** ***Confidentiality*:** Ensures that secret information or data is never disclosed to unauthorized devices.
- ***e.*** ***Integrity*:** Ensures that a message received is not

CONFERENCE PAPER

"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013

Organized by

Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

corrupted.

B. Challenges:

a. ***Channel vulnerability–*** broadcast wireless channels allow message eavesdropping and injection easily.
b. ***Node vulnerability–*** nodes do not reside in physically protected places, thus easily fall under attack.
c. ***Absence of infrastructure–*** certification/ authentication authorities are absent.

Dynamically changing network topology puts security of routing protocols under threat.

Power and computational limitations prevent the use of complex encryption algorithms.

II. SPREAD ARCHITECTURE

Several issues need to be addressed for SPREAD scheme in order to maximize the security. First, how do we divide the secret message into multiple pieces? Secondly, how the message pieces should be allocated onto each selected path? Thirdly, how do we discover the desired multiple paths in a MANET? We will briefly describe the first two issues as we have discussed them in other papers [2,3].

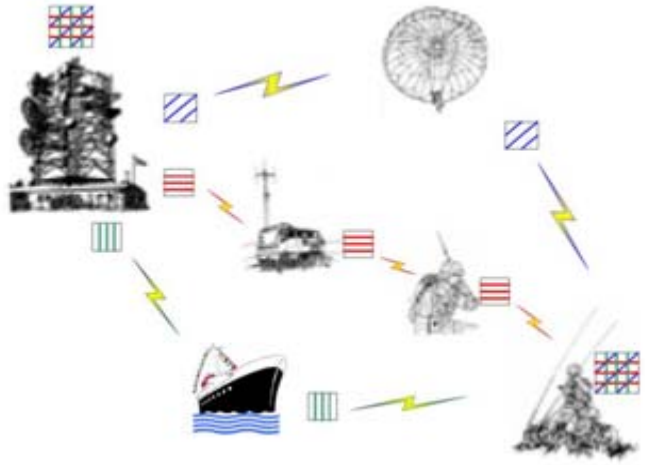

Figure 2: Illustration of SPREAD idea

A. Secret Sharing:

In our SPREAD scheme, we use the threshold secret sharing algorithm to divide the secret message into multiple pieces. Threshold secret sharing algorithms have been well studied in the literature. Assume that we have a system secret and we divide it into *N* pieces, called *shares* or *shadows*. Each of *N* participants of the system holds one share of the secret respectively. Any less than *T* participants cannot learn anything about the system secret, while with an effective algorithm, any *T* out of *N* participants can reconstruct the system secret. This is called a (*T*,*N*) *threshold secret sharing scheme.*

With a (*T*,*N*) secret sharing algorithm, the secret message can be divided into *N* message shares such that in order to compromise the message, the enemy must compromise at least *T* shares. With less than *T* shares, the enemy could learn nothing about the message and he has no better chance to recover the secret than an outsider who knows nothing at all about the message. The generation of the message shares and the reconstruction of the message are all linear operations over a finite field. The computational overhead is trivial ($O(Tlog2T)$). The detailed information on how to apply secret sharing algorithm in our SPREAD scheme can be found in [2].

B. Optimal Share Allocation:

The second issue is how to select the paths, how to choose an appropriate value of (*T*,*N*), and how to allocate the shares onto each selected path such that the maximum security can be achieved. The simplest and most intuitive share allocation scheme is to choose *N* as the number of available paths, apply (*N*,*N*) secret sharing, and allocate one share onto each path. This will achieve the desired maximum security with least processing cost. However, in an ad hoc network, wireless links are instable and the topology changes frequently. Sometimes packets might be dropped. In the case that packet loss does occur, this type of non-redundant share allocation will disable the reconstruction of the message at the intended destination. To deal with this problem, we introduce redundant (i.e. $T<N$) SPREAD scheme to improve the reliability. In [4] we discussed the optimal share allocations.

We formulated the share allocation into a constrained optimization problem, with the objective to minimize the message compromise probability. Our investigation to the optimal share allocation reveals that, by choosing an appropriate (*T*,*N*) value and allocating the shares onto each path carefully, we could improve the reliability by tolerating certain packet loss without sacrificing the security. The maximum redundancy we can add to the SPREAD scheme without sacrificing security is identified as $r \leq 1/m$

Where r=1-T/N *is* the redundancy factor and m is the number of paths selected to deliver the message. The optimal share allocation is proposed. Basically any allocation that conforms to the constraints

$$\begin{cases} N-T+1 \le n_i \le T-1, & i=1,\ldots,m \\ \sum_{i=1}^{M} n_i = N \end{cases}$$

Is an optimal share allocation in terms of security. More details about share allocation can be found in [15].

C. Multipath Routing:

Routing in ad hoc networks presents great challenge because the nodes in ad hoc networks can move freely and the topology changes continuously and unpredictably. A great effort has been made to design ad hoc routing protocols. Multipath routing technique is a promising choice since the use of multiple paths in a MANET could diminish the effect of unreliable wireless links and the constant topological changes. Several multipath routing schemes have been proposed to improve the reliability, fault-tolerance, end-to-end delay for bursty traffic, as well as to achieve load balancing etc. [5,6,7].

For our SPREAD scheme, we need independent paths, more specifically, node disjoint paths, because we are dealing with compromised node problem. Several multipath routing protocols have been proposed in MANETs with the design goal to find node-disjoint paths, such as the diversity injection

CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

technique [8], and the on-demand multipath routing [9]. The dynamic source routing protocol itself is also capable of maintaining multiple paths from the source to a destination. Those proposed protocols are all on demand, due to the network bandwidth limitation, and source routing type, as the source routing provides the source with the capability of controlling the disjointness of the paths. Those on-demand protocols work by broadcasting the route inquiry messages throughout the network and then gathering the replies from the destination and other nodes. Although those routing protocols are able to find multiple node-disjoint paths, the set of paths provided by them might not be optimal for our SPREAD scheme as the cost function they are based on is usually the hop count or propagation delay, not necessary the security.

For on-demand routing protocols, some type of cache is necessary to store the routes previously found so that the node does not have to perform the costly route discovery for each individual packet. In DSR[10] and the multipath extension of DSR, the route replies back to the source contain the complete node list from the source to the destination. By caching each of these paths separately, a "path cache" organization can be formed. This type of cache organization has been widely used. However, the paths found by this means might not serve our purpose best. They are not necessary the most secure paths. In [8], we designed an alternative cache organization, called a "link cache, in which routes are decomposed into individual links and represented in a unified graph data structure. Given the same amount of route reply information, the routes existing in a path cache can always be found in a link cache. Thus a link cache has the potential to use the route information more efficiently. We also developed an adaptive stale link removal scheme to work together with the link cache. By using such a link cache, we could separate the routing and the selection of the paths. Although we rely on an underlying routing protocol to provide us with a partial view of network topology, the selection of the optimal paths can be done orthogonal of the routing protocols used, based on the discovered partial network topology. In the next section, we present the maximal paths finding algorithm that is trying to select a set of paths, when used to deliver the message shares, providing the maximum overall security.

III. MAXIMAL PATHS FINDING ALGORITHM

Assume that we have totally *M* node-disjoint paths available. The security can be maximized when we allocate the shares in such a way that the enemy has to compromise all the *M* paths to compromise the necessary *T* shares. Here we assume that the enemy compromises shares by compromising nodes where the shares are relayed. We use *Pmsg*, the probability that the message might be compromised, to indicate the security of the SPREAD scheme. Then *Pmsg* can be calculated as follows,

Where *pi (i=1,2,…,M)* is the probability that path *i* is compromised, i.e., the probability that any intermediate node in path *i* is compromised.

Assume that with probability *qi* that node *ni* might be compromised. Then the probability that a (*s*,*t*) path consisting of node *s, n1, n2, …, nl, t* might be compromised equals to

$$p = 1-(1-q1)(1-q2)\ldots(1-ql)$$

Since we consider the protection of messages when they are transmitted across the network, we assume that the source and the destination are safe with *qs*= *qd*=0. Note that the probability *qi* indicates the security level of node *i* and it could be estimated from the feedback of some security monitoring software and/or hardware such as firewalls and intrusion detection devices. It could also be assigned manually by administrators based on the level of physical protection to nodes, the positions of nodes, or the rankings of nodes, etc.

D. Maximal node disjoint path finding algorithm:

Step 1. Find the first most secure path by modified Dijkstra algorithm, select the path

Step 2. Perform a graph transformation as follows for each selected path:

a. Replace the links used in the path with directed arcs – for the arc that is directed towards the source, make its cost the negative of the original link cost; make the cost of the arc directed towards the destination infinite (e.g. remove it)
b. Split each node on the selected paths (except the source and destination) into two collocated subnodes; connect the two subnodes by an arc of cost 0 and directed towards the source node.
c. Replace each external link that is connected to a node in the selected paths by its two component arcs of cost equal to the link cost – let one arc terminate on one subnode and the other one emanate from the other subnode such that along with the zero-cost arc, a cycle does not result.

Step 3. Run the modified Dijkstra algorithm, find the most secure path in the transformed graph

Step 4. Transform back to the original graph; erase any interlacing edges; group the remaining edges to form the new path set.

Step 5. Go to step 2, until no more path can be found or the security of the path set does not increase.

The maximal paths finding algorithm proposed for our SPREAD scheme is modified from the node disjoint shortest pair algorithm [11]. A modified Dijkstra algorithm is used so that negative links are allowed (but no negative loop) in the graph [11]. The modified Dijkstra algorithm modifies the standard Dijkstra algorithm by allowing the permanent labeled node change back to a tentative label when a smaller cost to that node is found. We define the following link cost function to convert the security characteristics into an additive link cost function so that the shortest path algorithm is readily used as most secure path finding algorithm.

We define the cost function of link between node *ni* and *nj* as

$$cij = -\log(1-qi)(1-qj)$$

Then the cost of the (*s*,*t*) path using shortest path algorithm is cost(s,t)=$c_{s1}+c_{12}+\ldots.+c_{ld}$

$=-\log(1-q_1)(1-q_2)-\ldots..-\log(1-q_1.)$

$=-\log[(1-q_1)(1-q_2)-\ldots..-(1-q_1))]$

With the shortest path algorithm,

cos t(s,t) is minimized

CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

$\Rightarrow$-log□ (1-q_1)(1-q2)-…..-(1-q_1))□ is minimized

$\Rightarrow$ (1-q_1)(1-q2)-…..-(1-q_1) is maximized

$\Rightarrow$ p=1-(1-q_1)(1-q2)-…..-(1-q_1) is minimized

So the path found by the shortest path algorithm would be the most secure path when the proposed cost function is used.

The maximal paths algorithm is then an iterative procedure. The most secure path is found first and added to the path set. Then in each iteration, the number of paths in the set will be augmented by one. Figure 2 summarizes the steps taken to find the maximal number of paths. Each time a new path is added to the set of selected paths, a graph transformation is performed, which involves a vertex splitting of the nodes on the selected paths (except the source and destination node). Then the modified Dijsktra algorithm is executed to find the most secure path in the transformed graph. Then by transforming the split nodes back to the original one, erasing any interlacing edges, grouping the remaining edges, the new path set is formed. In each iteration, the number of paths will be augmented by one.

Figure 3 shows an example of the path finding algorithm. After finding the first two node-disjoint paths, the third one temporarily makes use of the selected nodes but using the link in the reverse direction. After the interlacing removal and regrouping, a path set consisting of 3 paths is found instead of 2. Because of the regrouping of edges, the paths in the path sets in each iteration might change. So we calculate *Pmsg* after each iteration. If *Pmsg* is not getting smaller in the iteration, the path set found in the previous iteration will yield the best security results. The path finding algorithm terminates.

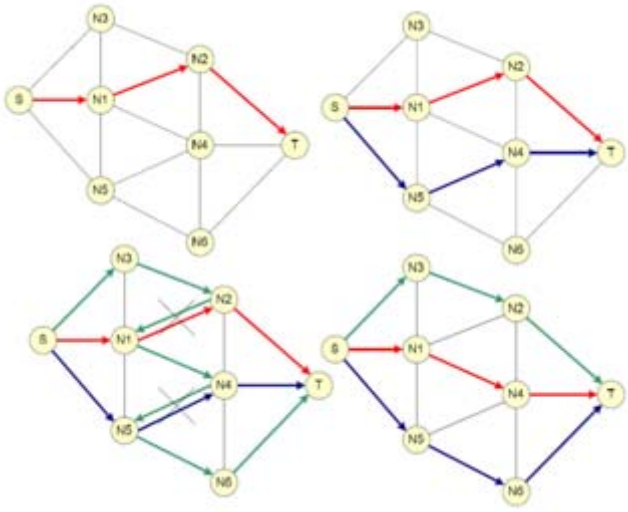

Figure 3: Illustration of the maximal node disjoint paths algorithm

IV. CLASSIFICATION OF ATTACKS

There are two types of security attacks:

– passive

– Active

In a passive attack, a malicious node either ignores operations supposed to be accomplished by it (examples: silent discard, partial routing information hiding), or listens to the channel, attempting to retrieve valuable information (example: eavesdropping).

In an active attack, information is inserted to the network and thus the network operation or some nodes may be harmed. Examples are impersonation/spoofing, modification, fabrication and disclosure attack.

In **Impersonation** attack, nodes may be able to join the network undetectably, or send false routing information, masquerading as some other trusted node. The Black Hole attack falls in this category: here a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. A more subtle type of routing disruption is the creation of a tunnel (or Wormhole) in the network between two colluding malicious nodes.

Routing-forwarding misbehaviors can be caused by nodes that are malicious or selfish. A malicious node misbehaves because it intends to damage network functioning. A selfish node does so because it wants to save battery life for its own communication by simply not participating in the routing protocol or by not executing the packet forwarding. To counter misbehavior, we can enforce cooperation. One way is to detect and then isolate misbehaving nodes through a watchdog and reputation mechanism. The watchdog identifies misbehaving nodes by performing neighborhood monitoring. Based on the information collected by the watchdog, the reputation system maintains a value for each node that represents the node's reputation. The reputation mechanism allows nodes to isolate misbehaving nodes by not serving their requests. Another way of countering misbehavior is to encourage nodes to cooperate and avoid selfish behavior through an incentive system.

V. TYPES OF SECURITY MECHANISMS

A. Preventive:

By using key-based cryptography, Key distribution is at the center of preventive mechanisms. Since no central authority, no centralized trusted third party, and no central server are available in ad hoc network, key management has to be distributed over the nodes.

B. The intrusion detection system (IDS):

In detective mechanisms has to monitor and rely on the audit trace that is limited to communication activities taking place within the radio range (i.e. partial and localized information).

VI. THE INTRUSION DETECTION SYSTEM (IDS)

A. Need for intrusion detection:

The use of wireless links renders a wireless ad-hoc network vulnerable to malicious attacks, ranging from passive eavesdropping to active interference. In wired networks however the attacker needs to gain access to the physical media e.g.: network wires etc. or pass through a plethora of firewalls and gateways. In wireless networks the scenario is much different, there are no firewalls and gateways in place

CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

hence attacks can take place from all directions. Every node in the ad-hoc network must be prepared for encounter with the adversary.

Each mobile node in ad-hoc network is an autonomous unit in itself free to move independently. This means a node with not adequate physical protection is very much susceptible to being captured, hijacked or compromised. It is difficult to track down a single compromised node in alarge network, attacks stemming from compromised nodes are far more detrimental and much harder to detect. Hence every node in a wireless ad-hoc network should be able to work in a mode wherein it trusts no peer.

Ad-hoc networks have a decentralized architecture, and many ad-hoc network algorithms rely on cooperative participation of the member nodes. Adversaries can exploit this lack of centralized decision making architecture to launch new types of attacks aimed at breaking the cooperative algorithms.

Furthermore, Ad-hoc routing presents more vulnerabilities than one can imagine, since most routing protocols for ad-hoc networks are cooperative by nature. The adversary who compromises an ad-hoc node could succeed in bringing down the whole network by disseminating false routing information and this could culminate into all nodes feeding data to the compromised node.

Intrusion prevention techniques like encryption and authentication can reduce the risks of intrusion but cannot completely eliminate them e.g.: encryption and authentication cannot defend against compromised nodes.

An IDS aims to enhance the intrusion prevention facility of the underlying security protocol. An ideal IDS should able to detect an anomaly quickly so that the misbehaving node/nodes can be identified and appropriate actions (e.g. punish or avoid misbehaving nodes) can be taken so that further damage to the network is minimized. It should be able to set thresholds for its detection schemes dynamically so that misbehaving nodes cannot easily work around the detection scheme. For detecting anomalies in packet forwarding it should not rely on overhearing packet transmissions of neighboring nodes since limitations on transmission range may make this impossible.

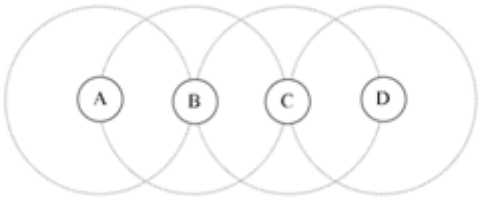

Figure. 4. Nodes in a network. Each dotted circle represents the transmission range of the corresponding node.

This lead to the following problematic situations:

a. ***Ambiguous collisions:*** A node will not be able to decode the contents of a packet by overhearing if the packet collides with other packets transmitted from other nodes. Hence a detection scheme based on overhearing may not be able to identify the nodes.
b. ***Receiver collisions:*** In receiver collisions a node *A* (in Figure 4) can tell if *B* has forwarded a packet to *C* but not if *C* has received it or not. Thus if *B* wants to circumvent the detection mechanism of *A*, it can purposefully cause a collision at *C* by forwarding the packet to *C* when *C* is transmitting.
c. ***Limited transmission power:*** A node *B* (in Figure 4) can limit its transmission power such that the transmitted signal is strong enough to reach the previous node *A* but not the actual recipient *C*.
d. ***Directional antennas:*** A directional antenna prevents neighboring nodes, that are not within its direction, from overhearing its transmissions.

B. General overview:

In general terms "Intrusion" is defined as "any set of actions that attempt to compromise integrity, confidentiality or availability of the resource".

The protocols and systems which are meant to provide services can be the target of attacks such as Distributed Denial of Service (DDOS). Intrusion detection can be used as a second line of defense to protect network systems because once an intrusion is detected response can be put in place to minimize the damage or gather evidence for prosecution or launch counter offensives.

Intrusion detection assumes that "user and program activities are observable ", which means that any activity which the user or an application program initiates, gets logged somewhere into system tables or some kind of a system log and intrusion detection systems (IDS) have an easy access to these system logs. This logged system/ user related data is called audit data. Thus, Intrusion detection is all about capturing audit data, on the basis of this audit data determining whether it is a significant aberration from normal system behavior, if yes then IDS infers that the system is under attack. Based on the type of audit data, IDS can be classified into 2 types viz.

a. Network based: Network based IDS sits on the network gateway and captures and examines network packets that go through the network hardware interface.
b. Host based: Host based IDS relies on the operating system audit data to monitor and analyze the events generated by the users or programs on the host.

C. Unsuitability of the Current IDS techniques for Ad-hoc paradigm:

Wireless ad-hoc networks don't have no fixed infrastructure, since almost all of current network based IDS sit on the network gateways and routers and analyze the network packets passing through them, this type of network based IDS are rendered ineffective for the wireless ad-hoc networks.

In case of wireless ad-hoc networks the only available audit data is restricted to the communication activities taking place within the radio range, and any IDS meant for these types of networks should be made to work with this partial and localized kind of audit data.

Anomaly Detection models of IDS cannot be used for wireless ad-hoc networks, since the separating line between normalcy and anomaly is obscure. A node that transmits

erroneous routing information (fabrication) can be either a compromised or is currently out of sync due to volatile physical movement. Hence in wireless ad-hoc networks it is difficult to distinguish between false alarms and real intrusions.

D. New proposed architecture:

IDS should be both distributed and cooperative to suit the needs of wireless ad-hoc networks. What is meant by this statement is that every node in the wireless ad-hoc network should participate in intrusion detection. Each node is responsible for detecting intrusion locally and independently but neighboring nodes can form an association and collaboratively investigate in a broader range.

Each node within the network has its own individual IDS agent and these agents run independently and monitor user and system activities as well as communication activities within the radio range. If an anomaly is detected in the local data or if the evidence is inconclusive, IDS agents on the neighboring nodes will cooperatively participate in a global intrusion detection scheme. These individual IDS agents constitute the IDS system to protect the wireless ad-hoc network.

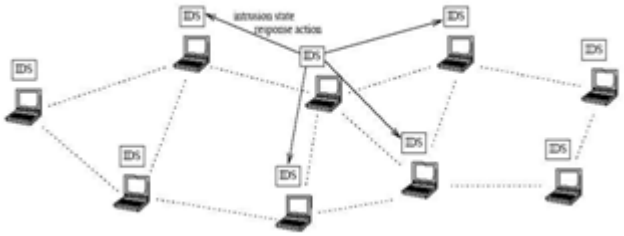

Figure 4: The IDS architecture for ad-hoc networks

E. IDS Agent:

A Typical IDS Agent consists of following modules viz.

a. Local Data Collection:

Local Data Collection module gathers streams of real time audit data from eclectic sources, which might include user and system activities within the mobile node, communication activities by this node as well as any communication activities within the radio range of this node and observable to this node.

b. Local Detection Engine:

Local detection engine analyzes the local audit data for evidence of anomalies. This requires the IDS to maintain some expert rules for the node against which the audit data collected would check. However as more and more appliances are becoming wireless, the types of planned attacks against these appliances is going to increase and this may make the existing expert rules insufficient to tackle these newer attacks. Moreover, updating these already existing expert rules is not a simple job. So any IDS meant for a wireless ad-hoc network should resort to statistical anomaly detection techniques. The normal behavior patterns called "Normal Profiles" are determined using the trace data from a "training "process where all activities are normal. During the "testing" process any deviations from the normal profiles are recorded if at all any occur. A detection module is computed from the deviation data to distinguish anomalies from normalcy. There are always going to be normal activities which have not been observed and recorded before, however their deviations from the normal profile is going to be much smaller than those of intrusions.

C. Cooperative Detection:

If a node locally detects a known intrusion with strong evidence it can very well on its own infer that the network is under attack and can initiate a response or a remedial action. However if the evidence of an anomaly or intrusion is a weak one or is rather inconclusive then the node decides it needs a broader investigation and can initiate a global intrusion detection procedure, which might consist of transmitting the intrusion detection state information among neighbors and further down the network if necessary.

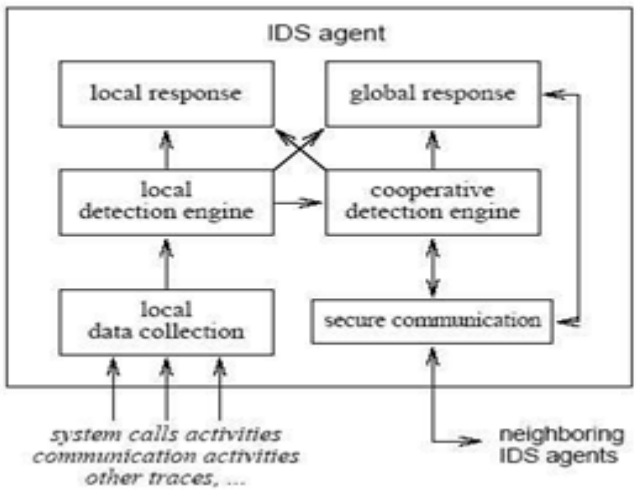

Figure 5: A Conceptual model for an IDS agent.

The intrusion detection state information may be a mere level-of-confidence value expressed as percentage.

a. With p% confidence, node A after analyzing its local data concludes that there is an intrusion.
b. With p% confidence, node A after analyzing the local data as well as that from its neighbors that there is an intrusion.
c. With p% confidence, node A, B, C,…. Collectively conclude that there is an intrusion.

To a more specific state that lists the suspects like,

d. With p% confidence, node A concludes after analyzing its local data that node X has been compromised.

A distributed consensus algorithm is then derived to compute the new intrusion detection state for the node under consideration, with the help of the state information recently received from the other nodes in the network. The algorithm might involve a weighted computation assuming that nearer nodes has greater effect than the far away ones.

A majority based Intrusion Detection Algorithm can include following steps:

a. The node sends to its neighboring node an "intrusion state request".

b. Each node, including the one which initiates this algorithm then propagates the state information, indicating the likelihood of an intrusion to its immediate neighbors.
c. Each node then determines whether the majority of the received reports point towards an intrusion, if yes then it concludes that the network is under attack.
d. Any node which detects an intrusion to the network can then initiate the remedial/response procedure.

As a rule of thumb, audit data from other nodes should not be trusted as compromised nodes might tend to send misleading data. However for compromised node sending audit data doesn't hold any incentives, in doing so it might create a situation which would result in its expulsion from the network. Hence, unless majority of nodes are compromised, and there exists at least one valid node the remedial procedure won't be initiated.

F. Intrusion response:

The type of intrusion response for wireless ad-hoc networks depends on the type of intrusion, the type of network protocols and the confidence in the veracity of the audit trace data. The response might range from resetting the communication channels between nodes or identifying the compromised nodes and precluding them from the network.

The IDS agent can notify the end user to do his/her own investigation and take the necessary action. It also sends re-authentication requests to all the nodes in the network, to prompt their respective end users to authenticate themselves. Only the re-authenticated nodes participate in negotiating a new communication channel and will recognize each other as legitimate nodes. Thus the malicious nodes can be precluded.

VII. CONCLUSION

We have presented an overview of the existing security scenario in the Ad-Hoc network environment. Key management, Ad-hoc routing and intrusion detection aspects of wireless Ad-hoc networks were discussed. Ad-hoc networking is still a raw area of research as can be seen with the problems that exist in these networks and the emerging solutions. The key management protocols are still very expensive and not fail safe. Several protocols for routing in Ad-hoc networks have been proposed. There is a need to make them more secure and robust to adapt to the demanding requirements of these networks. Intrusion detection is a critical security area. But it is a difficult goal to achieve in the resource deficient Ad-hoc environment. But the flexibility, ease and speed with which these networks can be set up imply they will gain wider application. This leaves Ad-hoc networks wide open for research to meet these demanding application. Finally, the SPREAD can be made adaptive in the sense that the source node could make final decision whether a message is delivered at certain time instant according to the security level and the availability of multiple paths. Moreover, the chosen set of multiple paths may be changed from time to time to avoid any potential capture of those multiple shares by adversaries.

VIII. REFERENCES

[1]. W. Lou, Y. Fang, "A survey on wireless security in mobile ad hoc networks: challenges and available solutions", book chapter in Ad Hoc Wireless Networking, to be published by Kluwer in May 2003

[2]. W. Lou, Y. Fang, "A multipath routing approach for secure data delivery", IEEE Milcom'01, Oct 2001

[3]. W. Lou, W. Liu, Y. Fang, "SPREAD: Improving network security by multipath routing", IEEE Milcom'03, Boston, MA, Oct 2003

[4]. W. Lou, W. Liu, Y. Fang, "SPREAD: Improving network security

[5]. Tsirigos, Z.J. Haas, "Multipath routing in the presence of frequent topological changes", IEEE Communication Magazine, Nov 2001

[6]. M.R. Pearlman, Z.J. Haas, P. Sholander, S. S. Tabrizi, "On the impact of alternate path routing for load balancing in mobile ad hoc networks", MobiHOC, 2000

[7]. K. Wu, J. Harms, "Performance study of a multipath routing method for wireless mobile ad hoc networks", 9th international symposium on modeling, analysis and simulation of computer and telecommunication system, 2001

[8]. W. Lou, Y. Fang, "Predictive caching strategy for on-demand routing protocols in ad hoc networks", Wireless Networks, vol.8, issue 6, Nov 2002

[9]. R. Bhandari, Survivable Networks – Algorithms for diverse routing, Kluwer Academic Publisher, 1999 by multipath routing", IEEE Milcom'03, Boston, MA, Oct 2003

[10]. D. B. Johnson, D. A. Maltz, Y.-C. Hu, and J. G. Jetcheva. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt, Apr. 2003.

[11]. M.R. Pearlman, Z.J. Haas, P. Sholander, S. S. Tabrizi, "On the impact of alternate path routing for load balancing in mobile ad hoc networks", MobiHOC, 2000

CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India