ISSN 2250-3153

# Mobile Wireless Network and Intrusion Detection

**Dr. Sameer Shrivastava**

Department of Computer Science and Engineering,
Global Nature Care Sanghatan Group of Institutions

***Abstract-*** An intrusion detection system framework for mobile wireless network is designed to support heterogeneous network environments to identify intruders at its best. The landscape of network security has drastically changed due to the rapid increase of wireless networks and mobile computing applications. Firewalls and encryption software methods have now become outdated for securing networks and are no longer sufficient and effective. There is a requirement for new architecture and mechanism to protect the wireless networks and mobile computing application.

In this paper, we will be examining the openness of wireless networks and put up an argument for inclusion of intrusion detection in the security architecture for mobile computing environment. We have developed such architecture and evaluated a key mechanism in this architecture, through simulation experiments.

***Index Terms***- intrusion detection, intrusion reply, mobile networks.

## I. INTRODUCTION

The landscape of network security has drastically changed due to the rapid increase of wireless networks and mobile computing applications. New vulnerabilities are created due to mobility which is not present in a fixed wired network, and so many of the proven security measures turn out to be ineffective. That is why, firewalls and encryption software are no longer sufficient for protecting networks. New architecture and mechanism is required to protect the wireless networks and mobile computing applications. The inference of mobile computing on network security research can be further confirmed by the follow case. Recently (Summer 2001) Windows-based server machines were attacked by an Internet worm called Code Red. To protect the internal networks from such type of worms many companies relied on firewalls. But then also, multiple incidents were reported of Code Red due to the use of mobile computers. Since there has been an increment in the usage of laptops and public venues (like conferences) providing wireless Internet access, there are higher and higher chances that an inadequately protected laptop will be infected with worms. For example, in a recent IETF meeting, amongst the hundreds of attendees who carried laptops, a dozens were detected to be infected with Code Red worm. And when these laptops are later incorporated back into their company networks, they spread the worms from within and let the firewalls become useless in defending this worm.

## II. SUSCEPTIBILITY OF MOBILE WIRELESS NETWORKS

It depends on the mobile computing environment which can make it very vulnerable for challenger's malicious attacks. Firstly, the use of wireless links leaves the network liable for attacks ranging from passive snoop to active prying. In wired networks an enemy must gain physical access to the network wires or pass through several lines of security at firewalls and gateways, the wireless network can be attacked from all directions and they can target at any node. Leaking secret information, message contamination, and node impersonation are usual damages done. All these mean that a wireless network will not have a clear line of security, and every node must be prepared for encounters with an enemy directly or indirectly.

Secondly, mobile nodes are independent units that are capable of wandering independently. Inadequate physical protection means that with are approachable to being captured, compromised, and hijacked. The tracking of a particular mobile node in a global scale network is not so easy, that is why attacks by a compromised node from within the network are far more damaging and difficult to detect. Therefore, no peer mode has to be prepared for mobile nodes and the infrastructure.

Thirdly, some wireless network algorithms rely on the cooperative participation of all nodes and the infrastructure for decision-making in mobile computing environment. No centralized authority means that the enemies can exploit for new types of attacks designed to break the cooperative algorithms.
For example, mostly the current MAC protocols for wireless channel access are weak. Although, most of MAC protocols have similar working principles, in a contention-based method, each node has to compete for control of the transmission channel every time it tries sending a message. Nodes should strictly follow the pre-defined method to avoid collisions and to recover from them. In a contention-free method, an exclusive use of the channel resource is seeks on a one-time or recurring basis for each node. MAC protocol type does not matter incase of a break down in a scenario resembling a denial-of-service attack, if a node behaves nastily. The wired networks have rarely Although these attacks because the physical networks and the MAC layer are isolated from the outside world by layer-3 gateways/firewalls, every mobile node is completely exposed in the wireless open medium.

To add on, new type of computational and communication activities are introduced in mobile computing that rarely appear in fixed or wired environment. For example, mobile users tend to be grudging about communication due to slow links, limited bandwidth, higher cost, and battery power constraints; means like disconnected operations and location-dependent functions only emerge to mobile wireless environment. Naturally, security

measures developed for wired network are likely incompetent to attacks that exploit these new applications.

Applications and services in a mobile wireless network can be a weak link as well. Possible attacks may target these proxies or agents running in base-stations and intermediate nodes to achieve performance gains through caching, content transcoding, or traffic shaping, etc to gain sensitive information or to mount DoS attacks, such as flushing the cache with bogus references, or having the content transcoder do useless and expensive computation.

To recapitulate, a mobile wireless network is vulnerable due to its features of open medium, dynamic changing network topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. Future research is needed to address these vulnerabilities.

## III. THE NEED FOR INTRUSION DETECTION

Intrusions can be reduced by preventive measures, such as encryption and authentication, but cannot be eliminated. For example, encryption and authentication cannot defend against compromised mobile nodes, which often carry the private keys. Integrity validation using redundant information (from different nodes), relies on the trustworthiness of other nodes, which could likewise be a weak link for sophisticated attacks such as those being used in secure routing.

Security research has a history that teaches us a valuable lesson that there are always some weak links that one could exploit to break in, no matter how many intrusion prevention measures are inserted in a network. Intrusion detection presents a second wall of protection and it is a necessity in any high secured network.

In short, mobile computing environment has intrinsic vulnerabilities that are not easily avoidable. To secure mobile computing applications, it is necessary to deploy intrusion detection and response system, and further research to be done to adapt these techniques to the new environment, likewise in fixed wired network. In this paper, we focus on a particular type of mobile computing environment called mobile networks and propose a new model for intrusion detection and response for this environment. We will first give a background on intrusion detection, then present our new architecture, followed by an experimental study to evaluate its feasibility.

## IV. PROBLEMS OF CURRENT IDS TECHNIQUES

It is rather difficult to apply current intrusion detection research used in fixed network into the mobile network. The difference comes into picture since the prior does not have a fixed infrastructure, and today's network-based IDSs, rely on real time traffic analysis, can no longer function well in the new environment. In wired networks where traffic monitoring is usually done at switches, routers and gateways, the mobile environment does not have such traffic focus points where the IDS can collect audit data for the whole network. Therefore, at any moment, audit trace available will be limited to communication activities taking place within the radio range, and the intrusion detection algorithms should be able to work on this partial and localized information.

The other noteworthy difference is in the communication pattern in a mobile computing environment. Mobile users tend to be grudging about communication and are prone to adopt new operation modes such as disconnected operations. This tells that the anomaly models for wired network cannot be used as is.

Furthermore, there cannot be a clear distinction between normalcy and irregularity in mobile environment.

A node sending out false routing information could be the one that has been compromised, or the one that is temporarily out of sync due to physical movement. Intrusion detection finds it difficult to distinguish between false alarms from real intrusions.

In short, our research must answer these questions in developing a feasible intrusion detection system for mobile networks:

- What is a good system architecture that fits features of mobile networks for building intrusion detection and response systems?
- What are the suitable audit data sources? How do we detect anomaly based on partial, local audit traces if they are the only dependable audit source?
- What is a good model of activities in a mobile computing environment that can separate anomaly when under attacks from the normalcy?

## V. INTRUSION DETECTION ARCHITECTURE

The needs of mobile network can be boosted by a suitable Intrusion detection and response systems which is both distributed and cooperative. In the architecture proposed, every node in the mobile network takes part in intrusion detection and response. Signs of intrusion can be detected locally and independently in each node, but neighboring nodes can collaboratively investigate in a broader range. Individual IDS agents are placed on each and every node from the systems aspect and run independently and monitors local activities. Intrusions are detected from local traces and response initiated. On the detection of an anomaly in the local data, or if the evidence is open to doubt and a broader search is warranted, neighboring IDS agents will cooperatively participate in global intrusion detection actions. These individual IDS agent collectively form the IDS system to defend the mobile network.

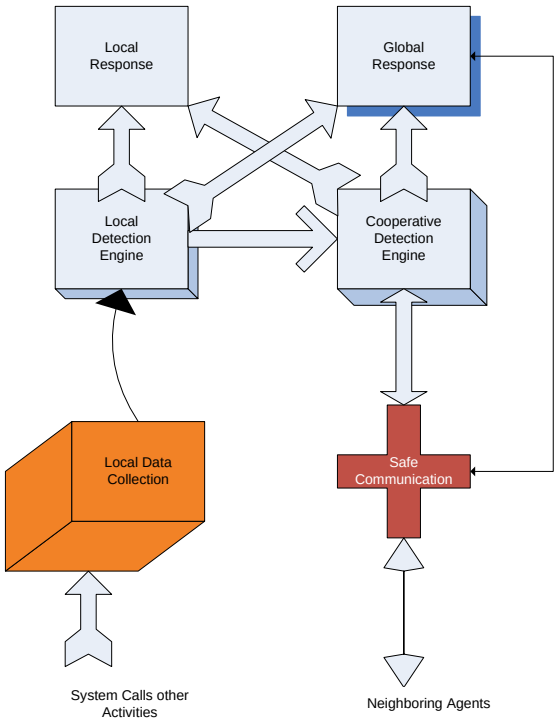


Fig. 1: An Intangible model for an Intrusion Detection System Agent

The internal of an IDS agent can be fairly complex, but theoretically it can be structured into six pieces (Figure 1). The data collection module is meant for gathering local audit traces and activity logs.

Next, to detect local anomaly the local detection engine uses this data. The cooperative detection engine is used in case of detection methods that need broader data sets or that require collaborations among IDS agents. The local response and global response modules are responsible for intrusion response actions. Actions local to this mobile node are triggered by the local response module, for example an IDS agent alerting the local user, while the global one synchronizes actions among neighboring nodes, such as the IDS agents in the network electing a remedy action. Finally, a secure communication module provides a high-confidence communication channel among IDS agents.

### *A. Data Collection*

The first module, local data collection, is meant for gathering streams of real-time audit data from various sources. Intrusion detection algorithms is used to decide, these useful data streams can include system and user activities within the mobile node, communication activities by this node, as well as communication activities within the radio range and observable by this node. Therefore, for a multi-layer integrated intrusion detection method multiple data collection modules can coexist in one IDS agent to provide multiple audit streams.

### *B. Local Detection*

The local detection engine is there to analyze the local data traces gathered by the local data collection module for evidence of anomalies. It can include both misuse detections and anomaly detection. Anomaly detection techniques will play a bigger role, since it is possible that the number of newly created attack types mounted on mobile computing environment will increase quickly as more network appliances become mobile and wireless.

### *C. Cooperative Detection*

Any node that detects locally a known intrusion or anomaly with strong facts, can determine independently that the network is under attack and can begin a response. However, if anomaly or intrusion with weak evidence is detected by a node, or the evidence is inconclusive but warrants broader investigation, it can begin a supportive global intrusion detection procedure. The working of the procedure is by propagating the intrusion detection state information among neighboring nodes. The intrusion detection state information can range from a mere level-of-confidence value such as

- With p% confidence, an intrusion is concluded by node A from its local data.
- With p% confidence, node A concludes from its local data and neighbor states that there is an intrusion
- With p% confidence, node A, B, C,... collectively conclude that there is an intrusion to a more specific state that lists the suspects, like
- With p% confidence, the compromise of node X is concluded by node A from its local data or to a complicated record including the complete evidence.

As the next step, it is possible to derive a distributed consensus algorithm to compute a new intrusion detection state for this node, using other nodes' state information received recently. The algorithm can take in a weighted computation under the assumption that nearby nodes has greater effects than far away nodes, i.e., giving the immediate neighbor the highest values in evaluating the intrusion detection states.

For example, a mostly distributed intrusion detection procedure can include the following steps:

- the node sends to neighboring node an intrusion (or anomaly) state request;
- each node (including the start node) then propagates the state information, indicating the likelihood of an intrusion or anomaly, to its immediate neighbors;
- each node then determines whether the majority of the received reports indicate an intrusion or anomaly; if yes, then it concludes that the network is under attack;
- any node that detects an intrusion to the network can then initiate the response procedure.

The rationales behind this scheme are as follows. Since, falsified data can be sent, so audit data from other nodes cannot be trusted and should not be used data. However, the compromised nodes have no incentives to send reports of intrusion/anomaly because the intrusion response may result in their removal from the network. Therefore, unless the majority of the nodes are compromised, in which case one of the legitimate nodes will probably be able to detect the intrusion with strong evidence and will respond, the above scheme can detect intrusion even when the evidence at individual nodes is weak.

A mobile network is considered highly dynamic because nodes can move in and out of the network. Therefore, while each node uses intrusion reports from other nodes, it does not rely on fixed network topology or membership information in the distributed detection process. It is a simple majority voting scheme where any node that detects an intrusion can initiate a response.

### D. Intrusion Response

The type of intrusion helps in deciding the response for mobile networks, the type of network protocols and applications, and the confidence (or certainty) in the evidence. For example, here is a few likely responses:

- Re-initializing communication channels between nodes (e.g, force re-key).
- Identifying the compromised nodes and reorganizing the network to preclude the promised nodes.

For example, the IDS agent can notify the end-user, who may in turn do his/her own investigation and take appropriate action, like can also send a re-authentication request to all nodes in the network prompting the end-users to authenticate themselves, using out-of-bound mechanisms. Only the re-authenticated nodes will be recognized as legal if, they collectively negotiate a new communication channel. That is, the compromised/nasty nodes can be excluded.

## VI. MULTI-LAYER INTEGRATED INTRUSION DETECTION AND RESPONSE

Unlikely, IDSs uses data only from the lower layers: network-based IDSs analyze TCP/IP packet data and host-based IDSs analyze system call data. This is due to application layer firewalls preventing many attacks, and application specific modules, e.g., credit card fraud detection systems, developed to guard the mission-critical services in wired networks.

In the wireless networks, to protect the services from attack there are no firewalls. However, intrusion detection in the application layer is not only feasible, but also necessary. Certain attacks, for example, an attack that is trying to create an unauthorized access back-door to a service, may seem perfectly legal to the lower layers, e.g., the MAC protocols. Our belief is that some attacks may be detected much earlier in the application layer, due to the richer semantic information available, than in the lower layers. For example, in case of a DoS attack, the application layer may detect quickly that operations don't make sense or a large number of incoming service connections have no actual operations; whereas the lower layers, relying only on information about the amount of network traffic, may take a longer time to recognize the extraordinarily high volume.

We need to synchronize the intrusion detection and response efforts, given that there are vulnerabilities in several layers of mobile wireless networks and that an intrusion detection module needs to be placed at each layer on each node of a network. We use the following integration scheme:

- if a node detects an intrusion that aspects the entire network, e.g., when it detects an attack on the routing protocols, it initiates the re-authentication process to exclude the compromised/nasty nodes from the network;
- if a node detects a local intrusion at a higher layer, e.g., when it detects attacks to one of its services, lower layers are noticed. The detection modules can then further investigate.

In this approach, though the detection on one layer can be commenced by evidence from other layers, but the intrusion detection module at each layer still needs to function properly. As a first cut of our experimental research, we will be allowing the evidence to flow from one layer to its (next) lower layer by default based on the application environment.

The amplified versions of the detection model at a lower level are constructed in such a manner that in the testing process, the anomaly decision, i.e., either 1 for yes or 0 for no from the upper layer is inserted into the deviation score of the lower level, for example, (0.1, 0.1) now becomes (0.1, 0.1, 0). In other words, the extra information passed from the upper level is by deviation data. The bodies of evidence from the upper layers and the current layer are mingled in case of an anomaly detection model built from the augmented data and can make a more informed decision. The intrusion report also comprises a vector of the information from the layers sent to other node for cooperative detection.

With the changes done, the lower layers now need more than one anomaly detection model: one that is relying on the data of the current layer and is using evidence from the lower layers, and the augmented one that also considers evidence from the upper layer.

We are able to achieve better performance in terms of both higher true positive and lower false positive rates, because, multi-layer combination enables us to analyze the attack scenario in its entirety and as a result. For example, a likely attack scenario is that a foe takes control of the mobile unit of a user, and then uses some system commands to send fallacious routing information. The global detection and response can immediately be initiated by detecting the event when a detection module that monitors user behavior, e.g., via command usage is used, which can result in the exclusion of this compromised unit. As another example, suppose the users are responding to a fire alarm, which is a rare event and may thus cause a lot of unusual movements and hence updates to the routing tables. Though, if there are no indications that a user or a system software has been compromised, each intrusion report sent to other nodes will have a clean vector of upper layer indicators, and thus the detection module for the routing protocols can conclude that the unusual updates may be genuine.

## VII. EXPERIMENTAL RESULTS

To study the feasibility of our security architecture, we have conducted a series of experiments to evaluate the effectiveness by implementing anomaly detection in a network simulator. Three specific wireless protocols were chosen as the subjects of study. They are Dynamic Source Routing (DSR) protocol, On-Demand Distance Vector Routing (ODV) protocol, and Destination-Sequenced Distance-Vector-Routing (DSDV) protocol; which were selected since they represent different types of wireless routing protocols, proactive and on-demand. Further we shall discuss how our anomaly detection methods can be applied to these protocols and then shall demonstrate the effectiveness of the models used on other different scenarios.

We used the wireless networks simulation software, from Network Simulator ns-21. It includes simulation for wireless network infrastructure, popular wireless routing protocols (DSR, DSDV, ODV and others), and mobility scenario and traffic pattern generation.

### A. Features Selection

The decision to pick features relies on several factors, like the reaction of information from several sources, i.e, from traffic pattern, from routing change, and from topological movement. A similar feature has been set for all so that we can compare among different protocols. Generally to allow slight deviation to make utmost utilization of routing information, we regard same sets for traffic and topological information. Even under the same gauge, different protocols infer it in a slight different way. For instance, PCH is the percentage of change in number of total intermediate hops from all source routes cached in DSR, but the percentage of change of sum of metrics to all reachable destinations in DSDV and ODV.

### *B. Models*

Two classification algorithms were used to build models, the traditional induction based classifier RIPPER and a new SVM classifier SVM Light. First, the models are trained online using training data from one of our simulations with pure normal data with running time of 100,000 seconds.

### *C. Data*

To test the models, five different test scripts were used to generate traces. normal is a normal trace, 100k-rt and 10k-rt are traces with intrusions on routing logic and with running time as 100,000 and 10,000 seconds respectively. 100k-tf and 10k-tf are traces with distortion on traffic patterns. 10k-rt and 10k-tf contain at most 10 intrusion sessions, while 100k-rt and 100k-tf contain at most 100 intrusion sessions. Then all results were altered through post-processing procedure. For each result, we run ten times and report its average and error under 95% confidence levels.

### *D. Discussion*

The experiment results demonstrate that on different wireless networks, an anomaly detection approach can work well, and so, the normal behavior of a routing protocol can be recognized and used to detect anomalies. First, it is important to point out that some spurious errors during normal use period were removed using a post-processing scheme. Though errors are inevitable in normal traces but we assume that they should not happen frequently. In contrast, numerous disorders are usually recorded during purposeful intrusion. On selection of a good window size, high false positive rate can be avoided and still high detection rate can be achieved. The intrusion detection research community can debate on how to detect an intrusion that relies on single plan. For example, on use of network connection data, the anomaly detection can be successful against multi-connection-based port scan and DDoS attacks, but then for a single-connection-based buyer-overflow attack, it is not so. Though, anomaly detection models can be very useful against buyer-overflow attacks if we use system call trace generated by a running program. Depending on, at which layer the data is collected there are some natural limits on detection capabilities. Similarly, for the routing protocols layer, our belief is that with the help of IDS on other layers, on the whole anomaly detection performance can be improved.

In this experiment, we also conclude that the normal behavior can be changed heavily by a few system parameters. One of them is the mobility level, which can lead to much higher alarm rate if the model is classified using values from another mobility level, which can further be resolved by randomizing the mobility level in the experiment. Though, the current ns-2 code is not in support for this feature. It however teaches us an important lesson that a good anomaly detection model should collect all possible value groupings and normal scenarios. Our plan is to develop schemes that shall cluster and categorize the normal scenarios by which we can build specific anomaly detection models for every normal scenario.

## VIII. CONCLUSION

We have argued that any secure network will have susceptibility that a rival could exploit. This is especially true for mobile wireless networks. To secure the mobile computing environment, intrusion detection can support intrusion prevention techniques (like encryption, authentication, secure MAC, secure routing, etc.). Still, to make intrusion detection work better for wireless networks a need is there for development of new techniques.

Through our ongoing investigation, which shows architecture for better intrusion detection in mobile computing environment should be distributed and cooperative. Intrusion detection and response mechanism have a critical component of anomaly detection. Trace analysis and anomaly detection should be done hand in hand in each node and if possible through cooperation with all nodes in the network. Moreover, intrusion detection should happen in all networking layers in an integrated cross-layer manner, though our focus of research was on routing protocols since they are the foundation of a mobile network. We projected the usage of anomaly detection model constructed using information available from the routing protocols for intrusion detection purposes. We have tried proving the performance by simulations. Finally, we showed that these detectors in general have good detection performance.

There were some interesting findings, like; we noted some difference in security performance amongst different types of routing protocols. We assert that protocols with strong correlation among changes of different types of information tend to have better detection performance. Especially, since the behavior of on-demand protocols reflects the correlation between traffic pattern and routing message flows, the on-demand protocols usually work better than table-driven protocols.

## REFERENCES

[1] M. Cagalj, S. Capkun, and J.-P. Hubaux, “Wormhole-Based Anti-Jamming Techniques in Sensor Networks”, in IEEE Transactions on Mobile Computing, January 2007

[2] Patwardhan, J. Parker, M. Iorga, A. Joshi, T. Karygiannis, Y. Yesha, Threshold-based intrusion detection in ad hoc networks and secure AODV, Ad Hoc Networks 6 (2008) 578–599.

[3] [42] S.A. Razak, S.M. Furnell, N.L. Clarke, P.J. Brooke, Friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks, Ad Hoc Networks 6 (2008) 1151–1167

[4] N. Komninos, C. Douligeris, LIDF: layered intrusion detection framework for ad hoc networks, Ad Hoc Networks 7 (2009) 171–182.

[5] Idika, N. & Mathur P. A., “A Survey of Malware Detection Technique”, In Proceeding of Software Engineering Research Center Conference, SERC-TR286, 2007.

## AUTHORS

**First Author** – Dr. Sameer Shrivastava, Associate professor, Global Nature Care Sangathan group of institutions, Jabalpur, M.P. India. His areas of specialization include Network Security. He is a Cisco Certified Network Associate, SUN certified and Microsoft Certified Professional.