SECURITY SOLUTIONS BY DETECTING FRAUDULENT USAGE IN WIRELESS NETWORKS

A.Sanjeeva Raju [1], A.Vanitha [2], A. Shylaja [3] and A.Ravi kumar [4]

[1]Assistant Professor, Department of CSE,
Kamala Institute of Technology & Science, Huzurabad, Karimnagar, AP, INDIA.
sanjeevaraju@rediffmail.com
[2]Assistant Professor, Department of IT,
Kamala Institute of Technology & Science, Huzurabad, Karimnagar, AP, INDIA.
vanitha_akinapalli@yahoo.co.in
[3]Assistant Professor, Department of MCA,
Sree Chaitanya Institute of Mgmt & Computer Sciences, Karimnagar, AP, INDIA.
shylaja_akinapally@rediffmail.com
[4]Student of M.Tech (CSE),
Sree Chaitanya College of Engineering, Thimmapur, Karimnagar, AP, INDIA.
ravikumar.akinapally@gmail.com

Abstract

Security research in to wired networks indicates that there are always some weak points in the systems that are hard to predict. This is particularly true for a wireless network, in which open wireless transmission media and low physical-security protection of mobile devices pose additional challenges for prevention-based approaches and detection-based approaches. Sensor network security mechanisms can be divided into two categories: communication protocols and key management architectures. Communication protocols deal with the cryptographic algorithms used to achieve availability, confidentiality, integrity, and authentication. Key management architectures handle the complexities of creating and distributing keys used by communication protocols. In this we explore Taxonomy of security solutions, Taxonomy of key distributing schemes, Detecting Computer and Network Misuse, Monitoring misuse through expert systems, Anomaly-based Intrusion Detection Using Mobility Profiles of Public Transportation Users, How to Increase Security in Mobile Networks by Anomaly Detection, The Baye's Decision Rule.

Keywords

Wireless Sensor Networks, Fraud, Intrusion detection, Wireless Ad Hoc Network, , Group Key Management Protocol.

1. INTRODUCTION

The Association of Certified Fraud Examiners (ACFE) defined fraud as "the use of one's occupation for personal enrichment through the deliberate misuse or application of the employing organization's resources or assets [1]. In the technological systems, fraudulent activities have occurred in many areas of daily life such as telecommunication networks, mobile communications, on-line banking, and E-commerce. Fraud is increasing dramatically with the expansion of modern technology and global communication, resulting in substantial losses to the businesses. Consequentially, fraud detection has become an important issue to be explored.

Fraud detection involves identifying fraud as quickly as possible once it has been perpetrated. Fraud detection methods are continuously developed to defend criminals in adapting to their strategies. The development of new fraud detection methods is made more difficult due to the severe limitation of the exchange of ideas in fraud detection. Data sets are not made available and results are often not

disclosed to the public. The fraud cases have to be detected from the available huge data sets such as the logged data and user behavior. At present, fraud detection has been implemented by a number of methods such as data mining, statistics, and artificial intelligence. Fraud is discovered from anomalies in data and patterns.

Telecommunication Fraud:

Fraud is costly to a network carrier both in terms of lost income and wasted capacity. The various types of telecommunication fraud can be classified into two categories: subscription fraud and superimposed fraud. Subscription fraud occurs from obtaining a subscription to a service, often with false identity details, with no intention of paying. Cases of bad debt are also included in this category. This fraud includes several ways, for example, mobile phone cloning, ghosting (the technology that tricks the network in order to obtain free calls), insider fraud, tumbling (rolling fake serial numbers are used on cloned handsets so that successive calls are attributed to different legitimate phones), and etc.

In general, the objective of fraud detection is to maximize correct predictions and maintain incorrect predictions at an acceptable level. A high correct diagnostic probability can be implied by minimizing probability of undetected fraud and false alarms. Some technical terms are described as follows. False alarm rate (or false positive rate) is the percentage of legitimate transactions that are incorrectly identified as fraudulent. Fraud catching rate (or true positive rate or detection accuracy rate) is the percentage of fraudulent transactions that are correctly identified as fraudulent. False Negative rate is the percentage of fraudulent transactions that are incorrectly identified as legitimate. In a fraud detection system, it is important to define performance metrics carefully. Several fraud detection techniques use metrics like the detection rate, false alarm rate, and average time of detection. The typical fraud detection techniques attempt to maximize accuracy rate and minimize false alarm rate.

Generally speaking, the following two complementary classes of approaches exist to protect a system: prevention- based and detection-based approaches. Security research into wired networks indicates that there are always some weak points in the systems that are hard to predict. This is particularly true for a wireless network, in which open wireless- transmission media and low physical-security protection of mobile devices pose additional challenges for prevention-based approaches. For example, although security measures are taken into account in the designs of second-generation (2G) and third- generation (3G) digital cellular systems, security flaws keep being reported in the literature [1]–[3]. One of the basic threats is the illegitimate use of services, which can lead to the problem of improper billing and masquerading and can cause drastic damage to service providers. Therefore, in order to provide defense-in-depth security mechanisms, a multilayer/multilevel protection system is necessary. Serving as the first level of protection schemes, prevention-based approaches (such as authentication and encryption) can effectively reduce attacks by keeping illegitimate users from entering the system. However, if a device is compromised, all the secrets associated with a device become open to attackers, rendering all prevention- based techniques helpless and resulting in great damage to the whole system. At this time, intrusion detection systems (IDSs), serving as the second level of protection schemes, if well designed, can effectively identify malicious activities and help offer an adequate protection for the system.

We aim at designing practical intrusion detection techniques for cellular mobile networks. We focus on users' calling and mobility activities because they represent two of the most important components of mobile users' profiles. Specifically, to utilize users' calling activities, we first apply the Chebyshev inequality to eliminate obvious malicious calls. This can lead to a reduced number of false alarms. We then formulate the intrusion detection problem as a multifeature two-category pattern-classification problem. Call duration time (CDT), call inactivity period (CIP), and call destination (CD) are extracted to form a feature vector to reflect users' calling activities.

A model of anomaly detection based on Bayesian decision rule is introduced, and its performance is discussed in terms of false positive and detection rates. To utilize users' mobility activities accurately and effectively, we first propose a realistic network model integrating geographic road-level granularities. The proposed network model takes into account both users' moving patterns and an actual location management scheme in the current cellular system; i.e., whenever a user crosses a boundary of a location area (LA), a location update operation is performed. Based on this model, we

present an instance-based-learning (IBL) technique to construct users' movement profiles. A similarity measure is defined to compare a user's activity with its constructed normal profile. A threshold policy is then used to decide whether the current activity is normal or not.

2. STATE OF ART

A. Security in Wireless Sensor Networks:

Rapid technological advances in the areas of micro electro-mechanical systems and miniaturization have spurred the development of a new kind of network. This network is composed of small, inexpensive sensors capable of intelligent sensing. Much research has been done with the aim of connecting large numbers of these sensors to create robust and scalable Wireless Sensor Networks (WSNs) on the order of hundreds of thousands of devices. Proposed applications for WSNs include habitat monitoring, battlefield surveillance, and security systems. Sensor devices, also called motes or nodes, typically consist of a sensing unit, a transceiver unit, a processing unit, and a power source unit.

Depending on the application, the sensing unit may monitor various types of data including acoustic, seismic, visual, and temperature data. The transceiver unit is a low-power radio capable of short range communication (tens of meters). The processing unit contains memory and a processor with severely limited size and speed. Wireless sensor motes are powered by a battery energy source which is not intended to be recharged. Designers hope to mass produce nodes for a very low cost per device (less than a dollar) and deploy them liberally as disposable devices. Communication usually consists of source nodes which sense the data and return it to sink nodes over multiple hops. Sink nodes may be ordinary sensor nodes or specialized base stations with greater resources.

Sensor network proponents envision a future in which thousands to millions of tiny sensor devices will be embedded in almost every aspect of life. The goal is to create intelligent environments capable of collecting massive amounts of information, recognizing significant events automatically, and responding appropriately. Sensor networks facilitate "large-scale, real-time data processing in complex environments" [Wood and Stankovic 2002]. Although military applications are the most obvious, sensor networks have potential in a wide range of arenas. Typical applications of the future might include emergency response information, energy management, medical monitoring, inventory control, and battlefield management [Perrig et al. 2001].If sensor networks are to attain their potential, however, secure communication techniques must be developed in order to protect the system and its users. The need for security in military applications is obvious, but even more benign uses, such as home health monitoring, require confidentiality. WSNs are ideal for detecting chemical, biological, or environmental threats over large areas, but maliciously induced false alarms could completely negate the value of the system. As Wood and Stankovic point out, if security is weak, sensor networks "will only be suitable for limited, controlled environments – falling far short of their promise." The widespread deployment and overall success of sensor networks will be directly related to their security strength.

- ***Sensor Security Challenges:***

The nature of large, ad-hoc, wireless sensor networks presents significant challenges in designing security schemes. Five of the most pronounced challenges are described below.

- ***Wireless Medium:***

The pervasive applications proposed for sensor networks necessitate wireless communication links. Furthermore, the ad-hoc deployment of sensor motes makes wired communication completely inappropriate. The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Although this problem is not unique to sensor networks, traditional solutions must be adapted to efficiently execute on sensor networks.

- ***Ad-Hoc Deployment:***

The ad-hoc nature of sensor networks means no structure can be statically defined beforehand. The network topology is always subject to changes due to node failure, addition, or mobility. Nodes may be deployed by air drop, so nothing is known of the topology prior to deployment. Since nodes may fail or be replaced the network must support self-configuration. Security schemes must be able to operate within this dynamic environment. Zhou and Haas maintain that "any security solution with a static configuration" will not suffice. The ever-changing nature of sensor networks requires more robust designs for security techniques to cope with such dynamics.

- ***Hostile Environment:***

A third challenging factor is the hostile environment in which sensor nodes function. Motes face the possibility of destruction or (perhaps worse) capture by attackers. Since nodes may be in a hostile environment, attackers can easily gain physical access to the devices. Attackers may capture a node, physically disassemble it, and extract from it valuable information (e.g. cryptographic keys). The highly hostile environment represents a serious challenge for security researchers.

- ***Resource Scarcity:***

The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. The radio operates at up to 40 Kbps bandwidth at a range of a few dozen meters. Such hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity, and memory. This is no trivial task. While energy is perhaps the most precious resource for sensor networks, previous work has given little to no attention to energy efficiency. Communication is especially expensive in terms of power. Clearly, security mechanisms must give special effort to be communication efficient in order to be energy efficient.

- ***Immense Scale:***

Finally, the proposed scale of sensor networks poses a significant challenge for security mechanisms. Simply networking tens to hundreds of thousands of nodes has proven to be a substantial task. Providing security over such a network is equally challenging. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency.

3. PROPOSED SOLUTIONS

While the majority of the research in sensor networks has focused on making them feasible and useful, a few researchers have proposed solutions to the security issues discussed previously. Sensor network security mechanisms can be divided into two categories: communication protocols and key management architectures. Communication protocols deal with the cryptographic algorithms used to achieve availability, confidentiality, integrity, and authentication. Key management architectures handle the complexities of creating and distributing keys used by communication protocols.

- ***Communication Protocols****:*

Currently there have been two major secure communication protocols proposed for sensor networks: SPINS [Perrig et al. 2001] and TinySec [Karlof, Sastry, and Wagner 2004]. Both protocols work at the link level to provide message confidentiality, authentication, and integrity using symmetric cryptography. The limited memory and CPU speeds of sensor nodes almost completely exclude the use of asymmetric cryptography sensor networks.

- ***SPINS :***

SPINS (Security Protocols for Sensor Networks) is comprised of two link layer protocols: SNEP and µTELSA. SNEP (Secure Network Encryption Protocol) provides data confidentiality, two-party authentication, and data freshness. The three patterns of communication in sensor networks: node to base station, base station to node, and base station to all nodes. SNEP handles the first two types, and

µTELSA handles the last. In order to minimize computation and memory requirements, SNEP bases all symmetric cryptographic primitives (encryption, message authentication code, hash, and random number generator) on the same block cipher, RC5. Another design goal is to minimize communication overhead. This is accomplished by reducing the packet overhead to 8 bytes and by storing state information instead of transmitting it with each packet.

SNEP supports data authentication, replay protection, and semantic security [Perrig et al. 2002]. Authentication is provided by calculating and appending a message authentication code (MAC) to each message. A MAC is essentially a cryptographically secure checksum [Karlof, Sastry, and Wagner 2004]. The MAC is recalculated upon reception and compared to the value in the transmission. To implement replay protection, SNEP requires a synchronized counter value at each node. The MAC is calculated using a secret key and the counter. As a result, out-of-sync packets will not be accepted. SPINS includes a counter exchange protocol for synchronizing counter values between two hosts. Although maintaining a synchronized counter adds significant overhead, it allows semantic security, a strong security property which assures that identical messages are encrypted differently each time they are encrypted. For example, if a sensor is simply reporting YES or NO regarding the occurrence of some event, an attacker may be able to discover the encrypted value of NO and subsequently be able to understand all encrypted transmissions. By encrypting the data based on the counter as well as the key, each NO will encrypt differently.

µTELSA, the second part of SPINS, provides authenticated broadcast for sensor networks. The goal of µTELSA is to allow base stations to transmit authenticated broadcasts to all of the nodes while preventing a compromised node from forging messages from the sender. µTELSA uses symmetric mechanisms to create an asymmetric system using a loosely synchronized clock. Receivers buffer broadcast packets until they receive the decryption key which is disclosed once in a specified time interval (epoch). The keys are calculated using a one-way hash function (F) and are disclosed in the reverse order that they are generated. Once a node receives a key, it can apply the same hash function to calculate the keys for previous epochs and decrypt buffered packets. Figure 1 illustrates this process.

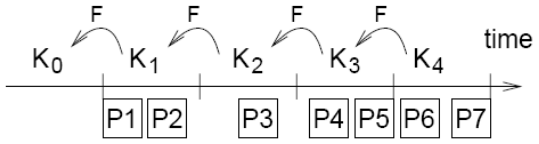

Figure 1: µTELSA key disclosure and computation.

Each hash mark denotes an epoch. P1, P2…P7 represent packets.

SPINS performs reasonably well according to its authors. Although key setup is expensive (4 ms), encrypting a 16 byte message and calculating its MAC only takes 2.5 ms. The limited bandwidth of the test platform, 10 kbps, allows time to perform key setup, encryption, and MAC calculation for every packet. The performance of µTELSA is bounded by the amount of buffer space available. Consequently, key disclosures must happen relatively frequently and must be reliably received.

The stated limitations of SPINS are that it does not completely deal with compromised nodes and it does not deal with denial-of-service attacks. SPINS merely ensures that a comprised node does not reveal the key to every node in the network. Additionally, SNEP needs tight synchronization of counters since they are not transmitted. Another design weakness is the dependence of µTELSA on buffering packets. The extremely limited storage space characteristic of sensors devices makes buffering particularly unattractive.

- ***Random Key Pre distribution:***

Another novel approach to key management is random key predistribution [Chan, Perrig, and Song 2003]. In this strategy, a random pool of keys from the key space is preloaded into each node. Two nodes must find a common key in their sets in order to communicate. A challenge-response protocol is used to verify that two nodes have a key in common. Chan, Perrig, and Song extend this basic idea

to a multipath-reinforcement scheme that strengthens the security between two nodes by exploiting the security of other links. Their work culminates in a random-pair wise key scheme which enables node-to-node authentication and quorum-based revocation. The strongest aspect of this strategy is that it provides complete resilience against node capture – a captured node reveals no information about the rest of the network.

- ***Security of Mobile ad-hoc Wireless Networks:***

In the past few years the wireless networks (WNs) reached a wide popularity because they satisfy an early but permanent human necessity: to communicate from everywhere, any time and everything. Thus, the major advantage that WNs offer is the mobility. That means people can stay connected to Internet outside their work office or home, in so called hot-spots available in an increasing number of locations as airports and coffee shops; within the work environment people can access the network in a more convenient mode, without the constrains of the wired networks. The mobility feature entails the increasing of productivity. In the same time the WNs have some advantages for network administrators: they are easy scalable, avoiding the problems involved by setting up additional cables and equipments. Often a wireless networks may be cheaper than his wired counterpart.

WNs found a lot of applications, civilian e.g. industry, environment monitoring, health care, traffic control, teleconferences, etc and military as well e.g. Enemy movement and activities surveillance, gathering information on radioactivity, chemical and biological contamination in battlefields, de-mining combat areas, etc. In WNs the devices can communicate in two different ways. First way, called peer to peer, allow direct communication among devices and no infrastructure is required. Two or more computers set to operate in peer to peer mode, each being within the rage of the other ones, are able to discover and communicate forming a wireless ad hoc network (WAHN). The second communication way relies on an infrastructure, like in cellular telephone systems. In this mode terminals cannot communicate directly but by means of a device which role is to control the network access and data traffic. From the security viewpoint the infrastructure based mode is more secure but is less versatile. Thus, many applications, especially military ones, cannot be implemented using this solution.

Powered by military researches, a special class of WAHNs has been developed: wireless sensor networks WSNs. There are many definitions of WSNs, among which we chose two [1]: National Research Council defined sensor networks as massive numbers of small, inexpensive devices pervasive throughout electrical and mechanical systems and ubiquitous throughout the environment that monitor and control most aspects of our physical world.

DARPA defined WSNs, as a deployment of massive numbers of small, inexpensive, self-powered devices that can sense, compute, and communicate with other devices for the purpose of gathering local information to make global decisions about a physical environment.

In a basic configuration, each node in a WSN comprises a microcontroller with memory support, one or more mode sensors and actuators, a transceiver and an energy source, typical a battery. Once deployed, devices start to self organizes and cooperate in order to accomplish a specific task. Unlike industrial WNs, which use standardized protocols, WSNs use specific protocols.

Mainly due to their unique characteristics:

- Small-scale sensor nodes
- Limited power they can harvest or store
- Harsh environmental conditions
- Node failures
- Mobility of nodes
- Dynamic network topology
- Communication failures
- Heterogeneity of nodes
- Large scale of deployment

Securing communications, in all WN types, is a major issue enforced by the nature of applications and transmission environment. Many laptops and PDA are lost or stolen every year creating security holes into enterprises' networks. In wireless sensors networks, operating in hostile environments, the nodes are vulnerable to capture and tamper. The information stored in the device may be read and, further the device may be used to compromise the network functionality. Both situations enumerated are arguments to be aware on the importance of the necessity to secure wireless networks.

4. SECURITY SOLUTIONS – STATE OF THE ART

A. Taxonomy of security solutions:

Security solutions for both WAHNs and WSNs may be classified on the communication model (peer to peer and group based), implementation layer (physical, network and application) and the technique used (cryptographic or non- cryptographic). Figure 2 shows the space of possible solutions. It is clear that non-cryptographic solutions are applicable only at physical layer, indifferent of what communication model is used. Cryptographic solutions are, on one hand, simpler to implement comparing with frequency hopping schemes– as non-cryptographic possible solution, and, on the other hand, are appropriate to any type of communication model and for both network and application layers.

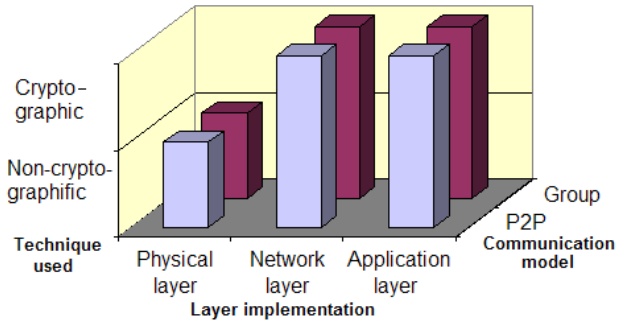

Figure 2: The space of possible security solutions

However, the approaches are substantial different for the two communication models. In peer to peer solution nodes establish pair-wise connections using some shared keys between each communicating nodes.

In group communication model nodes participate in a securely communication group whose members use a common group key to encrypt/decrypt group traffic. This implies the establishment of a communication group and the distribution of the group key(s) to each group member. The simplest solution is to use Traffic Encryption Key (TEK), but it is not suitable for dynamic groups because any membership change requires the group key refreshment.

B. Taxonomy of key distributing schemes:

In the past decade some researches were focused on finding appropriate protocols for group key management able to perform member identification and authentication, access control and key generation, distribution and installation. Nowadays is broadly accepted the classification of key management protocols in three important categories [9], [10]:

1. Centralized group key management protocols, in these protocols a single Key Distribution Center (KDC) is employed for controlling the entire group.

2. Decentralized key management protocols, these protocols divide large groups of nodes into subgroups, each subgroup having its own key management; the goal is to minimize the concentration of the problem in a single place.

3. Distributed key management protocols these protocols avoid using any explicit KDC, the problem of key management being solved by the group members themselves. Each category has advantages and disadvantages as well, but each one is more or less suitable for a specific purpose.

Another classification takes into account the structure used for rekeying. Two structures are used: linear or simple rekeying and combinatorial. First ones involve a single key per user and distribute the TEK using that key as in Iolus [11], GKMP (Group Key Management Protocol) [12] or LKH [13]. The second ones, more suitable in adhoc wireless networks use different combination of cryptographic keys seeking to minimize the number of rekeying messages when members of the group live or join the group. Such system named Exclusion Basis System (EBS) was developed by Morales at all [14] and is used as a main component of many key management solutions in WAHNS. However, it has some limitation in ad hoc networks that are described below:

Duplication of group management functions. In the current architectures the multicast session and group membership is kept at the network layer since the group security and key management problems are solved at application layer. Hence it follows the necessity of an increased computational effort and the need for consistency of management between the two layers. Moreover WAHNs' network layer cannot implement the multicast functionality as well as Internet. The latest approaches try to concentrate all these functionality at the application layer, with no network-level multicast support Overhead of distributing control traffic. Current key management protocols use the network-level multicast channel to distribute data and traffic control. It follows that all group members receive all rekeying messages, even if only a small subset of members need them. Hence the necessity of improved key management architectures that distribute the keys only to required nodes.

- ***Security and trust:***

In WAHNs the nodes are autonomous and decide they self if participate or not in group management. Moreover, the nodes may become selfish or, worst, may collude by exchanging rekeying information.

For sensor networks, the protocols used for implementing a group key management may be also classified according to the way the key are updated or not after nodes deploying. From this point of view we distinguish static and dynamic keying schemes. In static schemes, as that proposed by Eschenauer and Gligor, each node is assigned for k keys from P pool of keys in the phase of pre-deployment. The nodes in the neighborhood may establish a secure communication only if they share at least one key. This condition is provided with some probability by the proper selection of k and P. The main advantage of this scheme is the exclusion of the base station in the process of key management. Because the scheme is vulnerable to the node capture, an enhancement has been proposed by Chan; in this scheme the neighboring nodes may securely communicate if they share q keys, q<k.

Dynamic schemes changes all keys revealed to the attacker on the node capture, hence its major advantage compared to the static schemes related to the node capture. Due to the complexity dynamic key management, actual implementations mainly rely on a centralized key server.

Factors that affect GKMP solutions: There are many factors that influence the design of a GKMP; they may be grouped by the nature of the issues:

• Group-related factors includes the group size –the number of nodes within a group may vary from tens to ten thousands or more, group dynamics – consequence of the nodes mobility that may randomly join or leave the group and group structure and sub-grouping capability arising from the difficulty of rekeying a large number of nodes in a flat group.

• Network-related factors follow from the particularities of WAHNs that make them quite different from the wired networks: unreliable communication, less support for multicasting, different configuration and the factor of mobility.

C .Monitoring misuse through expert systems:

Expert systems provide strategies and mechanisms for processing facts regarding the state of a given environment, and deriving logical inferences from these facts. With respect to intrusion detection, a fact maps to an event that is recorded and evaluated by the expert system. Forward-chaining expert systems are well-suited for reasoning about activity within an event stream.

A forward-chaining rule-based system is data-driven: each fact asserted may satisfy the conditions

under which new facts or conclusions are derived. Alternatively, backward-chaining systems employ the reverse strategy; starting from a proposed hypothesis they proceed to collect supportive evidence. Backward- chaining systems are typically applied to problems of diagnosis, whereas forward-chaining strategies dominate systems involving prognosis, monitoring, and control applications. Using a forward-chaining rule-based system, one may establish a chain of rules, or rule set, with which a series of asserted facts may lead the system to deduce that a targeted multistep scenario has occurred. Within an intrusion detection system, event records are asserted as facts and evaluated against penetration rule sets. As individual rules are evaluated against facts and satisfied, the individual event records provide a trail of reasoning that allows the user to analyze the evidence of malicious activity in isolation from the full event stream.

- ***Anomaly-based Intrusion Detection Using Mobility Profiles of Public Transportation Users:***

Mobile wireless networks continue to be plagued by theft of identity and intrusion. Both problems can be addressed in two different ways, either by misuse detection or anomaly-based detection. Misuse detection is carried out by recognizing instances of well known patterns of attacks. The main limitation of this approach is that the system fails to uncover new kinds of attacks unless it has been instructed to do so. Anomaly- based intrusion detection (ABID) consists of observing and recognizing deviations from normal behavior, which has been captured and maintained in electronic profiles. It is generally acknowledged that the main limitation of the anomaly-based detection approach is that it generates a higher rate of false positives than the misuse detection approach.

The limitation imposed by anomaly-based detection approach can be minimized by combining observations across time and across domains. The use of different profiles for ABID has been investigated by various groups. Node/device profiles are created by exploiting the unique hardware signature of their wireless interface [6], operating system (proposed by Taleck [7]) and other characteristics of a wireless device. In terms of user- based profiling, the use of calling patterns for fraud detection in cellular networks is explored by Boukerche et al. [8]. Calls are classified into the normal category or anomalous category based to whether or not the time and location of the calls match the profile of the user. If the probability of fraud is high, then a warning message is sent to the client who owns the phone.

Commercial systems, namely the Fraud Management Sys- tem by Hewlett-Packard (FMS-HP) [9] and Compaq (FMS- C) [10] also make use of service usage profiles, which are built using calling patterns, call frequency, call times and duration, wireless home/roaming behavior and other call- related information. Although both FMSs offer some services, which permit them to be differentiated, they both detect multiple types of fraud by examining all calls (e.g. streams of call detail records used for billing purposes) and other-related events (event records).

- ***How to Increase Security in Mobile Networks by Anomaly Detection:***

Cellular radio networks gain more and more popularity and the amount of mobile communication will increase dramatically in the near future. Mobile users will no longer be restricted to the use of mobile phones. New network architectures like UMTS will place enhanced multimedia communication at the user's disposal. One major concern for the present and future cellular radio networks is security. But with increasing complexity of the networks the task of detecting, repulsing and preventing abuse by out and insiders becomes more and more difficult. Obviously it is not possible to make any system absolutely secure with the currently known security techniques like e.g. authentication and encryption. This is related to the fact that a lot of attacks are simply based on software flaws and design errors, which may often be intelligently combined in order to open the door to any system under attack. One recent example is the cloning of GSM cards [4].

Additional countermeasures are therefore needed. One possible technique is anomaly detection based on the profiling of mobile users. Anomaly detection tries to detect the abnormal use of a system, i.e. a behavior which is significantly different from the usual behavior of a user. It is not restricted to any specific network environment. As a matter of fact, an anomaly detection component is a major building block within most available intrusion detection systems (IDS).

D. Anomaly Detection

The first work in the field of anomaly detection has been done over a decade ago, focusing on main frame scenarios. With the rise of more complex data and telecommunication networks like the Internet and mobile networks the designers of anomaly detection systems have to face new challenges resulting from the more distributed nature of these networks, lists three main statistical models currently used for anomaly detection:

- operational model
- The mean and standard deviation model
- time series model

The operational model is based on thresholds, i.e. an alarm is raised if a variable observed (e.g. the number of login attempts) reaches a certain threshold. The mean and standard deviation model raises an alarm if an observation does not lie within a given confidence interval. The time series model takes the time at which an event takes place into account. If the probability for that event at that particular time is too low an alarm is raised.

Anomaly detection systems have major advantages compared to other intrusion detection approaches as they:
1. Do not require any a priori knowledge of the target system, and
2. Provide a way to detect unknown attacks.
But there also exist serious disadvantages which have to be considered before applying any of these techniques:

1. Not all users actually have a normal or standard behavior.
2. A user can slowly change his behavior over time from “good” to “bad”, i.e. fool the system by slow long term attacks.
3. The privacy of the users can be seriously injured.

First of all we introduce our general approach towards anomaly detection, which is based on the Baye’s rule.

E. The Baye’s Decision Rule

The approach towards anomaly detection is based on the Baye’s decision rule and can therefore be classified as a statistical approach. The Baye’s decision rule is widely used in statistical pattern recognition [6]. A pattern recognition problem can be described in the following way: A set of objects can be divided into a number of classes. For each of these objects we measure a couple of observable characteristics and combine them to a vector. This observation vector will be different for each object, thus we can interpret this vector as a random variable X. To classify a new object, we have to learn the probability distribution of X for each class. If we know these distributions, we can calculate the probability that an object with observation vector x belongs to class c, namely P(cjx). Therefore we can classify a new object in the following way:

1. Measure the observation vector for the object.
2. Calculate the class probabilities P(cjx) for every class.
3. Choose the class with the highest probability as the object’s class.

This decision rule is called the *Baye’s decision rule for minimum error rate*. It can be shown that every other decision rule yields even higher error rates than the Baye’s rule. The so-called *a-posteriori* probability P(cjx) can be expressed as:

$$P(c|x) = \frac{P(c)p(x|c)}{p(x)}$$

p(xjc) is the *class conditional* probability density of observing a vector x, P(c) is the *a-priori* probability for class c, and p(x) is the probability density of observing a vector x. Because p(x) is constant for every class c for a particular observation vector x, all we have to do is to learn the class conditional probability density p(xjc) and the a-priori probability P(c). P(c) can be calculated as the

relative frequency of observing a vector of class c. E.g. if we observe n vectors and n1 vectors of them are of class c1, the empirical probability ^ P(c1) can be calculated as

$$\hat{P}(c_1) = \frac{n_1}{n}$$

p(xjc) is more difficult to learn. A simple technique is the use of histograms: We divide the vector space into intervals, count the number of vectors falling into every interval and then estimate the probability of vectors within this interval as the proportion of the number of vectors within this part compared to the number of all vectors. This technique only works if the number of intervals is small compared to the number of vectors (e.g. low dimension of the vector space).

5. CONCLUSION

We have investigated Fraudulent Usage in Wireless Networks & Security Solutions for Wireless Networks. We formulate the intrusion detection problem as a multi feature two class pattern-classification problem and apply to exploit movement patterns demonstrated by mobile users. Although there are many security protocols that have been proposed for cellular mobile networks, how to design a highly secure cellular mobile network still remains a very challenging issue due to open radio-transmission environment and physical vulnerability of mobile devices.

ACKNOWLEDGMENTS

The authors would like to thank the reviewers for their useful comments that greatly improved the presentation and clarity of this paper.

REFERENCES

[1] B. Sun, F. Yu, K. Wu, Y. Xiao, and V. C. M. Leung, "Enhancing security using mobility-based anomaly detection in cellular mobile networks," *IEEE Trans. Veh. Technol.*, vol. 55, no. 4, pp. 1385–1396, Jul. 2006.

[2] Y.-B. Lin, M. Chen, and H. Rao, "Potential fraudulent usage in mobile telecommunications networks," *IEEE Trans. Mobile Comput.*, vol. 1, no. 2, pp. 123–131, Apr.–Jun. 2002.

[3] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 734–742, Mar. 2005.

[4] H. Debar, M. Dacier, and A. Wespi, "A revised taxonomy for intrusion detection systems," *Ann. Telecommun.*, vol. 55, no. 7/8, pp. 361–378, 2000.

[5] D. E. Denning, "An intrusion-detection model," *IEEE Trans. Softw. Eng.*, vol. SE-13, no. 7, pp. 222–232, Feb. 1987.

[6] B. Sun, F. Yu, K. Wu, and V. C. M. Leung, "Mobility-based anomaly detection in cellular mobile networks," in *Proc. ACM WiSe Conjunction ACM Mobicom*, Philadelphia, PA, 2004, pp. 61–69.

[7] U. Lindqvist and P. A. Porras, "Detecting computer and network misuse through the production-based expert system toolset (P-BEST)," in *Proc. IEEE Symp. Security Privacy*, Oakland, CA, May 1999, pp. 146–161.

[8] S. Kumar and E. Spafford, "A pattern matching model for misuse intrusion detection," in *Proc. 17th Nat. Comput. Security Conf.*, Oct. 1994, pp. 11–21.

[9] K. Ilgun, "USTAT: A real-time intrusion detection system for unix," in *Proc. IEEE Symp. Res. Security Privacy*, Oakland, CA, May 1993, pp. 16–28.

[10] H. Debar, M. Becker, and D. Siboni, "A neural network component for an intrusion detection system," in *Proc. IEEE Symp. Res. Security Privacy*, Oakland, CA, May 1992, pp. 240–250.

[11] J. Hall, M. Barbeau, and E. Kranakis, "Anomaly-based intrusion detection using mobility profiles of public transportation users," in *Proc. IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun.*, Montreal, QC, Canada, Aug. 22–24, 2005, pp. 17–24.

[12] D. Samfat and R.Molva, "IDAMN: An intrusion detection architecture for mobile networks," *IEEE J. Sel. Areas Commun.*, vol. 15, no. 7, pp. 1373– 1380, Sep. 1997.

[13] H. A. Karimi and X. Liu, "A predictive location model for location-based services," in *Proc. 11th ACM Int. Symp. Advances Geographic Inf. Syst.*, New Orleans, LA, 2003, pp. 126–133.

[14] Y. Fang, I. Chlamtac, and Y. Lin, "Modeling PCS networks under general call holding time and cell residence time distributions," *IEEE/ACM Trans. Netw.*, vol. 5, no. 6, pp. 893–906, Dec. 1997.

[15] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification*, 2nd ed. Hoboken, NJ: Wiley, Oct. 2000.

Authors

A. Sanjeeva Raju received the Bachelor of Engineering Degree in computer science & engineering from Dr.Babasaheb Ambedkar Marathwada University, Aurangabad, Maharastra, India in 2001,the Master of Technology in computer science & engineering from the Jawaharlal Nehru Technological University, Hyderabad, Andhra Pradesh, India in 2010.
From 2001 to 2002, he was a Lecturer in Computer Science department at Dr.V.R.K college of Engineering & Technology, Jagtial, Karimnagar, Andhra Pradesh, India. Currently he is an Assistant Professor in Computer Science & Engineering department at Kamala Institute of Technology & Science, Singapur, Huzurabad, Karimnagar, Andhra Pradesh, India. His research interests are in the areas of information theoretic security, databases, and language technologies. He has guided more than 15 projects to the students of Bachelor of Technology course.
Mr.Sanjeeva Raju is a life member in Indian Society for Technical Education. He is JKC (Jawahar Knowledge Center) Coordinator; SPOC (Single Point Of Contact) to IEG (Institute for Electronic Governance).He is a Core Team Member for Infosys Foundation Program of Infosys Campus Connect. He is deputed as Observer, External Examiner, Chief Examiner, and Valuator for students of Bachelor of Technology.

Vanitha Akinapalli received the Bachelor of Technology Degree in computer science & information technology from Jawaharlal Nehru Technological University, Hyderabad, Andhra Pradesh, India in 2005,the Master of Technology in computer science & engineering from Jawaharlal Nehru Technological University, Anantapur , Andhra Pradesh, India in 2010.
From 2005 to 2006, she was a Lecturer in Computer Science & Engineering Department at Kamala Institute of Technology & Science, Singapur, Huzurabad, Karimnagar, Andhra Pradesh ,India. Currently she is an Assistant Professor in Information Technology Department at Kamala Institute of Technology & Science, Singapur, Huzurabad, Karimnagar, Andhra Pradesh, India. Her research interests are in the areas of information theoretic security, databases, and language technologies. She has guided more than 10 projects to the students of Bachelor of Technology course.
Ms.Vanitha is a life member in Indian Society for Technical Education. She is deputed as Observer, External Examiner, Chief Examiner, and Valuator for students of Bachelor of Technology.

Shylaja Akinapally received the Bachelor of Science Degree in computer science from Kakatiya University, Warangal, Andhra Pradesh, India in 2005,the Master of Computer Applications Degree from Jawaharlal Nehru Technological University, Hyderabad , Andhra Pradesh, India in 2008.
From 2008 to 2009, she was an Assistant Professor in Master of Computer Applications Department at Kamala Institute of Technology & Science, Singapur, Huzurabad, Karimnagar, Andhra Pradesh, India.
Currently she is an Assistant Professor in Master of Computer Applications Department at Sree Chaitanya Institute of Management & Computer Sciences, Thimmapur, Karimnagar, Andhra Pradesh, India. Her research interests are in the areas of information theoretic security, databases, and language technologies. She is deputed as Observer, External Examiner, Chief Examiner, and Valuator for students of Master of Computer Applications. She is also doing the Master of Technology Degree in Computer Science & Engineering at Sree Chaitanya College of Engineering, Thimmapur, Karimnagar, Andhra Pradesh, India.

Ravi kumar Akinapally received the Bachelor of Technology Degree in Information Technology from Sree Chaitanya College of Engineering, Thimmapur, Karimnagar, Andhra Pradesh, India in 2010, Doing the Master of Technology Degree in Computer Science & Engineering at Sree Chaitanya College of Engineering, Thimmapur, Karimnagar, Andhra Pradesh, India. His research interests are in the areas of information theoretic security, databases, and language technologies.