Survey on Wireless Intrusion Detection Mechanisms

Moble Jacob
TocH Institute of Science and Technology,
Arakkunnam

Rasmi P.S., PhD
TocH Institute of Science and Technology,
Arakkunnam

ABSTRACT

Wireless communication is technology's one of the promising contributions to mankind. Wireless networks are widely used to transfer sensitive data such as bank details, credit card details, emails etc nowadays. The intrusion detection system for wired network cannot be applied directly for wireless networks. Wireless network does not have specific boundaries since the nodes are moving. Wireless networks are more vulnerable to attacks such as denial of service, spoofing attacks, session hijacking etc. It is easy for the attacker to intrude into the system since no physical connection is needed. This paper deals with the survey of some of the methods used in intrusion detection in wireless network.

Keywords

Wireless intrusion detection, Dos attack, Management frames.

1. INTRODUCTION

Wireless network has many advantages over wired network such as flexibility, support of mobility of the nodes, easy to deploy, cost effective etc. Since the nodes are moving there is no specific topology in case of wireless networks. Wireless networks are susceptible to malicious attacks which ranging from passive attacks to active attacks. Encryption and authentication methods are used to prevent intrusion, but these methods cannot eliminate the problems. Most of the systems focus on the attacks which threaten confidentiality. In a wireless network the availability as well as integrity is also important.

The intrusion detection systems can be characterized either on the basis of the data being analyzed or on the basis of methods that are used to detect the attack. Based on the data being analyzed, the intrusion detection systems can be classified as the one which works on the data in the physical layer, the one which works on the data in the MAC layer or the system which works with the data from the physical as well as from the MAC layer. Based on the method used for intrusion detection, the systems can be classified as the one which uses misuse detection, the one which uses anomaly detection or the system which uses both systems.

The systems which take physical layer data for reference mainly focus on jamming attacks. Most of the systems use radio frequency fingerprinting or signal to noise ratio to detect the attacks. The systems which take MAC layer data as reference can detect attacks like MAC spoofing, denial of service, session hijacking, etc. There are systems which uses the physical layer data and the MAC layer data. In misuse detection, signatures of attacks were stored. The real time traffic is analyzed and compared with the signatures. If the analyzed traffic matches with the signature, the event is an attack otherwise the event is considered as a normal event.

In anomaly based intrusion detection, a normal model is created. The real time traffic is compared with the normal model. If the analyzed traffic matches with the normal model, the event is considered as a normal event otherwise it is considered as an abnormal event. The detection threshold can be adjusted so as to reduce the false alarms.

2. WIRELESS NETWORK ATTACKS

Attacks can be categorized as either active or passive. Active attacks involve in altering of resources. Passive attacks do not involve in altering resources and are mainly a threat to the confidentiality. Wireless network attacks includes probing & network discovery, DoS attacks, impersonation, man in the middle attack etc. Most of the attacks were based on the physical layer as well as the data link layer. The physical layer deals with the radio signals. The data link layer deals with exchange of frames. Frames are of three types, data frames, control frames and management frames.

2.1 Physical Layer Attacks

In the physical layer there can be problems such as hidden terminal problem, capture effect. Hidden terminal problem occurs when a wireless node is visible from an access point, which are not visible from other nodes communicating with that AP. Capture effect is a phenomenon associated with signal reception in which only the stronger of two signals will be demodulated. Both phenomenons are caused due to concurrent transmissions and collisions at the receiver side. However, the important differentiation between the two is that the transmitting stations that are causing capture at the receiver are not necessarily hidden from each other.

2.2 Data Link Layer Attacks

In the data link layer, the data frames are encrypted in order protect the data from unauthorized exposure. The management frames are more prone to attacks. There are different DoS attacks such as authentication flood, deauthentication attack, association flood etc which exploit the management frames. In authentication flood attack, authentication requests are sending with spoofed addresses to the access point. At the access point, there is a client association table for each client with a limited size. The requests from the attacker add an entry to the association table. When the table reaches its limit, the legitimate user cannot authenticate and associate with the access point. The attacker spoofs the address of the victim and send deauthentication request which results in the disconnection of the victim from the access point. In case of association flood, the attacker exhausts the association table with huge number of spoofed association requests. Similar to authentication flood, the legitimate user cannot connect with the access point when the association table overflows.

3. WIRELESS INTRUSION DETECTION MECHANISMS

MOJO [1] is a system which deals with the wireless anomaly detection based on the physical layer data. It proposes a fine grained algorithm which is capable of distinguishing the root causes of wireless anomalies. It detects the hidden terminals and differentiates it with the capture effect. In wireless network, there will be interference from other devices such as microwave ovens, cordless phones. It detects noise from other non-WLAN devices, anomalous signal strength variations at access points and the variation of signal strength due to the environmental changes or due to the actions of access point. The signal strength is monitored in each beacon in order to detect abnormal signal strength variations. Faults are observed at different sensors and correlating information is needed from different distributed sniffers. The system provide detailed information about the faults occur at the physical layer.

In wireless LAN, MAC address can be easily spoofed. MAC address spoofing can be detected using received signal strength (RSS) [2]. The system proposes an approach based on Gaussian mixture model (GMM) to built RSS profile for detecting MAC address spoofing. Spoofing methods mainly focus on MAC headers since MAC layer encryption is only applied to the payload. Spoofing can be detected by analyzing the sequence number field. It is difficult to match attacker's sequence number to the legitimate device's sequence number. There are some open-source drivers and reverse-engineered firmware which allows per-frame SN manipulation. Almost all fields in MAC layer can be spoofed. But physical layer information is inherent to radio characteristics. Due to advancements in wireless devices the RSS based detection technique is not efficient. RSS profiling algorithm is proposed based on Expectation-Maximization learning for GMM. The significant changes in profiled RSS pattern is considered as spoofing attack.

Wireless Network Security can be improved Using Spectral Fingerprints [3]. The system use radio frequency fingerprints for classification to provide hardware specific identification for detection and mitigation of spoofing. The power-based RSS metric statistics may vary under different conditions such as different physical environments or in case of different hardware. The functionality of radio fingerprinting is divided into four steps. They are Waveform parameter extraction (amplitude and phase), Transient detection (preamble starting location), Feature Extraction (RF fingerprint), Classification of unknown received signals. Among these transient detection is the core functionality. Transient detection reliability is addressed using a Variance Trajectory technique with instantaneous amplitude and phase responses. Then the Power Spectral Density features from signal preamble are extracted to form RF fingerprint. Reference fingerprints are generated from signals from various devices. The unknown signals can generate its fingerprint and classified by correlating it with the reference fingerprints.

Spoofing and Anomalous Traffic can be detected in Wireless Networks via Forge-Resistant Relationships [4]. The system proposes a non cryptographic mechanism for authentication as well as to detect spoofing. The authentication requires key management or maintenance which is not possible in case of wireless LAN. Full-scale authentication has the risk of authentication key to be compromised and requires an infrastructure to maintain integrity of authentication methods. The system provides a lightweight security solution for authentication and it detects multiple devices which use same network identity. The system detects anomaly behavior within the MAC layer. The system verifies the forge-resistant relationships between packets which are coming from the claimed identity. There are two relationships which are taken into account in this system. They are relationships that are introduced through auxiliary fields in packets and relationships that result from the use of intrinsic properties associated with the transmission and reception of packets. There are two approaches that use auxiliary fields. They are Anomaly Detection via Sequence Number Monotonicity and One-Way Chain of Temporary Identifiers. The approaches that use intrinsic properties are Traffic Arrival Consistency Checks and Joint Traffic Load and Interarrival Time Detector. Even though the attacker spoofs any identity it can be easily detected using relationships.

DOMINO [5] is a system to detect greedy behavior in IEEE 802.11 hotspots. The wireless internet service providers provide different security mechanisms. The wireless node needs to be authenticated at the access point. There should be mechanisms to detect the greedy behavior of wireless nodes. A station can attain the bandwidth at the expense of other stations misusing the MAC protocol. The key features of the system are integration with the access point without interfering with the normal functionalities, compatibility with existing networks and applicability to future versions. During monitoring the traffic traces of sending stations are collected at regular intervals of time called monitoring periods. The traced data are analyzed using the DOMINO algorithm. In order to reduce false positives there is a threshold beyond which the suspect is considered as a cheater. In order to reduce the erroneous detection the cheat count will be decremented each time the station does not cheat. There are different tests being done to the traced data. The systems checks whether the station transmits before its required DIFS period after its last acknowledgement. Then it checks for oversized NAV value followed by backoff manipulation, actual backoff and consecutive backoff. Each test keeps its local counter and if it exceeds the threshold the remaining tests are aborted to save resources and the station is considered as cheater.

Effective and robust detection of jamming attacks [6] deals with the wireless anomaly detection based on the physical layer data. Two types of algorithms were proposed. One is locally executed algorithms and other is fusion algorithms. In locally executed algorithms, signal to noise ratio is measured. Statistical changes in SNR are monitored and algorithm executed independently. In fusion algorithms the locally executed results are combined to form a collaborative output. Local detection algorithms are categorized into two, simple threshold algorithms and cumulative sum change point detection algorithms. The algorithms consider SNR-based metrics which include the average SNR, minimum SNR, and max-minus-min SNR, in a short window. The values of these metrics are measured over a small time window and during a large time window another metric is compared. When the considering metric deviates from the normal or expected value, the simple threshold algorithms trigger an alarm. The normal value is the value of the metric estimated in a long time window. A collaborative intrusion detection system (CIDS) system collects and fusses information from the monitors and takes final decision about a possible attack. Depending on the output of the locally executed algorithms, several types of fusion algorithms can be used such as average, product, majority vote etc.

Multilevel monitoring and detection system (MMDS) [7] is based on an agent based monitoring in different levels. Different rules were generated using fuzzy decision support system. The system provides a framework based on hierarchical security agent. A security node consists of agents such as Manager Agent, Monitor Agent, Decision Agent, and Action Agent. The Manager Agent coordinates the activities such as sensing, communicating, and generating responses of agents. The security issues of the monitored environment are addressed by performing a unique function at each agent. In case abnormalities or intrusion, Decision Agent can take a robust decision with the help of fuzzy inference engine which provide imprecise and heuristic knowledge since between the normal and abnormal activities are not distinct but rather fuzzy. The action agent reports the state of the monitored environment and generates alerts, heartbeats, etc. The necessary action is taken by Action Agent such as killing a process, block potential intruder from accessing the user, alerting the administrator about the intrusion, etc. The system detects ssh attacks, nmap attacks and MAC spoofing attacks. The system only allows offline training.

Multiple spoofing attackers can be detected and the location can be identified in wireless networks [8] using spatial correlation with the received signal strength. Number of attackers can be determined using cluster based mechanism. Support vector machine is used to improve accuracy of number of attackers. The main contributions are GADE (generalized attack detection model) and IDOL: an integrated detection and localization system. Attack detection is done in the generalized attack detection model by using partitioning around medoids. A mechanism called SILENCE is used to improve the accuracy of determining the number of attackers.

The wireless intrusion mechanisms and its features are summarized in the Table 1.

Table 1. Wireless intrusion detection mechanisms and features

Sl. No.	Method	Physical/ Data link layer	Features
1	Mutual Observation with Joint Optimization (MOJO)	Physical layer data	•Detect capture effect and hidden terminals with the help of signal strength variation •Information from different sniffers were correlated
2	Detection of MAC address spoofing using RSS	Physical layer data	•RSS profile for the genuine stations were built based on Gaussian mixture model
3	Detection using frequency fingerprints	Physical layer data	•Power Spectral Density features from signal preamble are extracted to form RF fingerprint •Reference fingerprints are correlated with the unknown signals fingerprint
4	Detection using forge-resistant relationships	Data link layer data	•Relationships that can be introduced through auxiliary fields of packets and Intrinsic properties associated with the transmission and reception of packets were used
5	Detection using DCF inter-frame space (DIFS)	Data link layer data	•Used to detect greedy behavior of a station •Checks whether the station transmits before its required DIFS period after last acknowledgement
6	Detection using signal to noise ratio	Physical layer data	•Statistical changes in SNR are monitored & algorithm executed independently • Locally executed results are combined to form a collaborative output in fusion
7	Multilevel Monitoring and Detection System (MMDS)	Data link layer data	•Provides hierarchical security agent framework • Security node consists of Manager Agent, Monitor Agent, Decision Agent, Action Agent • Disadvantage: only allows offline training
8	Detection using spatial correlation with the RSS	Physical layer data	•Detect both spoofing attacks & number of attackers • Clustering based on RSS-based spatial correlations among normal devices and attackers

4. CONCLUSION

Wireless communication networks become an inevitable medium for communication nowadays. Wireless network are more prone to attacks such as spoofing, denial of service etc. These attacks can be detected using different detection systems which make use of data from physical layer, MAC layer or the data from both layers. This paper deals with some of the methods which detect intrusion. The methods take data from the wireless network, then process it and detect the intrusion. The problem in detecting the intrusion is that the accuracy of the system is based on the training of the system in case of anomaly detection systems. In case of signature based systems, all possible attack signatures should be stored in order to get better performance. Some methods works offline that is the previously collected data is used for detection and the real time traffic cannot be analyzed. In order to improve the performance of the wireless intrusion detection system, it is better to take care of possible frame loss which may tend to occur during the online evaluation and context dependency during the training phase.

5. REFERENCES

[1] A. Sheth, C. Doerr, D. Grunwald, R. Han, and D. Sicker, “MOJO: a distributed physical layer anomaly detection system for 802.11 WLANs”, in Proceedings of the 4th international conference on Mobile systems, applications and services, June 19-22, 2006, Uppsala, Sweden.

[2] Sheng, Y., Tan, K., Chen, G., Kotz, D. and Campbell, A. “Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength”, in Proceeding IEEE 27th Annual Conference on Computer Communications (INFOCOM), April 2008.

[3] W.M.Suski II, M.A.Temple, M.J.Mendenhall, and R.F.Mills, “Using spectral fingerprints to improve wireless network security”, in proceedings of the IEEE Global Communications Conference (GLOBECOM), December 2008.

[4] Q. Li, and W. Trappe, “Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationships”, Information Forensics and

Security, IEEE Transactions on , vol.2, no.4, pp.793-808, Dec. 2007.

[5] M. Raya, J.P. Hubaux, and Imad Aad, “DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots”, in Proceedings of the 2nd international conference on Mobile systems, applications, and services (MobiSys '04), ACM, New York, NY, USA.

[6] A.G.Fragkiadakis, V.A.Siris, and A.P.Traganitis, "Effective and robust detection of jamming attacks". Future Network and Mobile Summit, 2010, vol., no., pp.1-8, 16-18 June 2010.

[7] D. Dasgupta, F. Gonzalez, K. Yallapu and M. Kaniganti, “Multilevel monitoring and detection systems (MMDS)”, in Proceedings of the 15th Annual Computer Security Incident Handling Conference, Ottawa, Canada, 2003.

[8] J. Yang, Y. Chen, W. Trappe, J. Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks", Parallel and Distributed Systems, IEEE Transactions on , vol.24, no.1, pp.44,58, Jan. 2013.