Intrusion Detection in Mobile Adhoc Network with Bayesian model based MAC Identification

Bhagyashali Kokode, Prof. Mukul Pande, Prof. Sarvesh V. Warjurkar

Abstract: Mobile Ad-hoc Networks (MANETs) are a collection of heterogeneous, infrastructure less, self-organizing and battery powered mobile nodes with different resources availability and computational capabilities. The dynamic and distributed nature of MANETs makes them suitable for deployment in extreme and volatile environmental conditions. They have found applications in diverse domains such as military operations, environmental monitoring, rescue operations etc. Each node in a MANET is equipped with a wireless transmitter and receiver, which enables it to communicate with other nodes within its wireless transmission range. However, due to limited wireless communication range and node mobility, nodes in MANET must cooperate with each other to provide networking services among themselves. Therefore, each node in a MANET acts both as a host and a router. Present Intrusion Detection Systems (IDSs) for MANETs require continuous monitoring which leads to rapid depletion of a node's battery life. To avoid this issue we propose a system to prevent intrusion in MANET using Bayesian model based MAC Identification from multiple nodes in network. Using such system we can provide lightweight burden to nodes hence improving energy efficiency.

***Keywords**: Mobile Ad hoc Network; IDS; Routing protocols; Attacks, MAC*

*****

I. INTRODUCTION

The dynamic and distributed nature of MANETs make them vulnerable to various types of attacks like black hole attack, traffic distortion, IP spoofing, DoS attack etc. Malicious nodes can launch attacks against other normal nodes and deteriorate the overall performance of the entire network [1–3]. Unlike in wired networks, there are no fixed checkpoints like router and switches in MANETs, where the Intrusion Detection System (IDS) can be deployed [4,5]. Therefore, nodes in MANETs must cooperate in many aspectsincluding intrusion detection for their well being [6–8]. IDSs have been deployed with great degree of success across diverse domains like wireless Ad-hoc networks [5,9], MANETs [10–12], wireless sensor networks [13], cyber-physical system [14], cloud computing [15], large scale complex critical infrastructures [16] etc.

In this paper, we focus on IDS for MANETs. Due to absence of any centralized monitoring entity in MANETs, each node runs its own IDS and usually operates in a promiscuous mode. However, owing to limited battery life, it is not feasible to keep the IDS running continuously on MANET nodes. Most of the current MANET IDS schemes do not take into account the nature of the environment they are operating in and therefore they end up monitoring all nodes with equal probability, irrespective of whether or not the node being monitored has a history profile of being malicious. This results in a poor monitoring strategy wherein the node operating the IDS ends up wasting most of its energy monitoring the normal nodes. Another issue with many MANET IDS schemes [17–19] is that they generate heavy intrusion detection related traffic. Unlike the wired networks, MANETs have limited bandwidth and therefore, a large amount of intrusion detection related traffic can cause severe congestion in the network and limit the flow of normal traffic. In addition, heavy intrusion detection traffic also leads to more energy consumption among MANET nodes for processing them. Designing a MANET IDS scheme that is energy efficient and generates a low IDS traffic, while at the same time maintaining a high accuracy and detection rate is an active area of research.

In this paper, we model the intrusion detection process in MANETs using a game theoretical framework. Game theory based MANET IDSs [20–22] have been found to be energy efficient as well as generate low IDS trafficthrough application of dynamic and economical monitoring strategies. Game theory based IDS models the intrusion detection problem as a non-cooperative game between two competing players (attacker and defender), where the defender player (cluster leader node) tries to maximize its payoff by increasing its probability of successful intrusion detection while the attacker player (malicious node) tries to minimize its probability of being detected by the IDS.

Game theory based IDS scheme allows the IDS to assess the type of the node being monitored and adopt appropriate monitoring strategies. Nodes are assigned maliciousness values based on the history profile of their observed actions. Unlike most conventional IDSs that adopt promiscuous monitoring strategy and results in high IDS traffic generation, game theory based IDS uses a dynamic monitoring strategy wherein nodes with high maliciousness values are monitored more frequently compared to nodes with low maliciousness values. This helps the IDS to conserve its energy and minimize the overall IDS traffic generation. In a game theoretic IDS framework, a rigorous monitoring strategy is adopted by the IDS if the environment it is operating in is hostile. On the other hand, if the environment is less hostile, a less rigorous monitoring strategy is adopted by the IDS.

II. RELATED WORK:

In this section, we provide a brief background study on different types of MANET IDS based on their detection mechanism and modes of operation. We then discuss about various intrusion detection issues in MANETs and analyze the related works which have been categorized into non-game theory based and game theory based. Finally, the drawbacks associated with the related works have been listed out which provides us with the motivation for our work to address them.

Shakshuki et al. [18] proposed an IDS named Enhanced Adaptive Acknowledgment (EAACK) for MANETs. Their scheme requires all acknowledgment packets to be digitally signed by its sender and verified by its receiver. They used DSA and RSA as digital signatures and showed that their scheme is able to detect wide range of attacks. However, the drawback of their scheme is the requirement to digitally sign all the acknowledgments which increases computational overhead.

Marti et al. [32] proposed an IDS scheme for MANET which consists of two different modules, viz. the Watchdog and the Pathrater. In this scheme, the Watchdog acts as an IDS for the MANET and detects malicious node behaviors in the network by promiscuously listening to its next hop's transmission. If the Watchdog notices that its immediate next node fails to forward the packet within a given period of time then it increments the node's failure counter. If the failure counter of the monitored node exceeds a threshold value then the Watchdog reports the node as misbehaving. The Pathrater is then employed to inform the routing protocol to avoid the reported nodes for further data transmission. The drawback of this scheme is that it requires continuous monitoring by the Watchdog for detecting intrusions.

Lui et al. [17] proposed a TWOACK MANET IDS scheme which requires every data packets transmitted over three consecutive nodes along the source to the destination path to be acknowledged. Every node along the route has to send back an acknowledgment packet to the node that is two hop counts away from it in the route. The arrival of TWOACK packet at first node X (in the three consecutive nodes along the route) indicates a successful transmission of packet from node X to node Z via the intermediate node Y. However, if this TWOACK packet is not received within a given predefined time interval, both nodes Y and Z are reported as malicious. The drawback of this scheme is that it introduces a routing overhead due to frequent TWOACK packet generation.

Misra et al. [33] proposed a distributed self-learning, energyaware and low complexity protocol for intrusion detection in wireless sensor network. Their protocol uses the stochastic Learning Automata (LA) on packet sampling mechanism to obtain an energy efficient IDS. They showed that their approach was successful in detecting and removing malicious packets from the WSN. The drawback of this scheme is that the LA needs multiple rounds of learning before it becomes efficient.

Haddadi and Sarram [34] proposed a hybrid IDS model for Wireless Local Area Network (WLAN) that uses both misuse and anomaly based IDS sub-modules to detect intrusion. The drawback of this approach is that the response times of the misuse based and anomaly based IDSs are different. It also introduces significant computational overhead due to processing of the same data traffic by two different IDSs. A light weight, energy efficient and non-cryptographic intrusion detection solution against the gray hole attack in MANET is proposed in Reference [35] by Mohanapriya and Krishnamurthi.

However, their scheme requires the IDS to operate in a promiscuous mode to detect intrusions, which results in high power consumption for operating the IDS. A game-theoretic solution for Ad-hoc networks that models the cooperation and selfishness of the networks are discussed in References [36,37].

In these schemes, each node decides whether to forward or not forward a packet based on the trade-offs involved in cost (energy consumption) and benefits (network throughput) involved in collaborating with other nodes in the network. Therefore, enforcing a cooperation mechanism ensures that a selfish node that does not obey the network rules receives a low throughput. The drawback of this scheme is that it assumes the complete information game, where nodes have full knowledge about the network parameters.

Lui et al. [19] proposed a game theoretic framework to analyze the interactions between pairs of attacking/defending nodes using a Bayesian formulation in wireless Ad-hoc Networks. They suggested a Bayesian hybrid detection approach for the defender, in which a less powerful lightweight module is used to estimate the opponent's type, and a more powerful heavyweight module acts as a last line of defense. They analyzed the obtainable Nash Equilibrium (NE) for the attacker/defender Bayesian game in both static and dynamic settings and concluded that the dynamic approach is a more realistic model, since it allows the defender to consistently update its belief about the maliciousness of the opponent player as the game evolves. The drawback of their work is that it is difficult to determine a reasonable prior probability about the maliciousness of the attacker player.

Liu [38] proposed a general incentive-based method to model attacker's intent, objectives and strategies (AIOS) based on game theoretic formalization. The author developed an incentive-based conceptual framework for

AIOS modeling which can capture the inherent inter-dependency between AIOS and defender objectives and strategies in such a way that AIOS can be automatically inferred. The AIOS modeling enables the defender to predict which kind of strategies are more likely to be taken by the attacker than the others, even before such an attack happens. The AIOS inferences lead to more precise risk assessment and harm prediction. The drawback of the scheme is that it assumes the complete information game.

Chen et al. [39] proposed a framework that applies two game theoretic schemes for economic deployment of intrusion detection agent. In the first scheme, the interaction between an attacker and the intrusion detection agent is modeled and analyzed within a noncooperative game theory setting. The mixed strategy Nash Equilibrium solution is then used to derive the security risk value. The second scheme uses the security risk value derived by the first scheme to compute the Shapley value of the intrusion detection agent while considering the various threat levels. This allows the network administrator to quantitatively evaluate the security risk of each IDS agent and easily select the most critical and effective IDS agent deployment to meet the various threat levels to the network. The drawback of this scheme is the computational overhead involved for calculating the Shapley values of the intrusion detection agents.

Agah et al. [20] and Alpcan and Basar [21] addressed the attack– defense problem in a sensor network as a two-player noncooperative, non-zero-sum game. In their model, the game is assumed to have a complete information and the payoff function of the opponent player decides each player’s optimal strategy. The drawback of their work is the assumption that the players have complete information about the game.

III. SUMMARY

In summary, we found that most of the non-game theory based IDS schemes proposed in the literature are computationally expensive and require continuous monitoring, thereby leading to more power consumption for operating the IDS. The game theory based IDSs proposed in the literature addresses this issue to some extent. However, most of the previous works on game theory based MANET IDS assumes a complete information game where both players (attacker and defender) have complete information about the game. But such an assumption is usually not valid in a real network, where each node only has a partial information about the network because all network parameters are not known a priori. We also found that most of the games are static in nature where the strategies and utilities of players are fixed and repeated over a period of time. This approach fails in a dynamic environment where players adopt different strategies at various stages of the game. We also found that most of IDSs proposed in literature for MANETs are specific to certain classes of attacks like blackhole attack, wormhole attack etc. [32,40]. All these drawbacks in the related works provide us with the motivation to propose a new MANET IDS scheme based on incomplete information game to address them.

Problem Statement

A sensor node has limitation in terms of computation capability and energy reserves.Method is prohibitively expensive in terms of communication overhead.The possibility of node compromise introduces more challenges because most of the existing in-network aggregation algorithms have no provisions for security.A compromised node might attempt to thwart the aggregation process by launching several attacks, such as eavesdropping, jamming, message dropping, message fabrication, and so on.

IV. PROPOSED SYSTEM

The proposed system can be described as following modular explanation.

Setting up Network Model

Our first module is setting up the network model. We consider a large-scale, homogeneous sensor network consisting of resource-constrained sensor nodes. Analogous to previous distributed detection approaches; we assume that an identity-based public-key cryptography facility is available in the sensor network. Prior to deployment, each legitimate node is allocated a unique ID and a corresponding private key by a trusted third party. The public key of a node is its ID, which is the essence of an identity-based cryptosystem. Consequently, no node can lie to others about its identity. Moreover, anyone is able to verify messages signed by a node using the identity-based key. The source nodes in our problem formulation serve as storage points which cache the data gathered by other nodes and periodically transmit to the sink, in response to user queries. Such network architecture is consistent with the design of storage centric sensor networks

Falsifying the local value:

A compromised node C can falsify its own sensor reading with the goal of influencing the aggregate value. We assume that if a node is compromised, all the information it holds will be compromised. We conservatively consider that all malicious nodes can collude or can be under the control of a single attacker. We use a Byzantine fault model, where the adversary can inject any message through the compromised nodes. Compromised nodes may behave in arbitrarily malicious ways, which means that the sub-aggregate of a compromised node can be arbitrarily generated. However, we assume that the attacker does not launch DoS attacks, e.g., the multi-hop flooding attacks with the goal of making the whole system unavailable.

Computing Sum Despite Attacks:

In this module, we develop an attack-resilient protocol which enables BS to compute the aggregate despite the presence of the attack. We observe that, in general, BS can verify the final synopsis if it receives one valid MAC for each '1' bit in the synopsis. In fact, to verify a particular '1' bit, say bit i , BS does not need to receive authentication messages from all of the nodes which contribute to bit i . As an example, more than half of the nodes are likely to contribute to the leftmost bit of the synopsis, while to verify this bit, BS needs to receive a MAC only from one of these nodes.

Performance Analysis

For the proposed system protocol, we use the following specific measurements to evaluate its performance:

- Deviation of Estimate
- Number of (Unique) MACs
- Average Nodes Sent bits

V. CONCLUSION

We discussed the security issues of in-network aggregation algorithms to compute aggregates such as predicate Count and Sum. In particular, we showed the falsified sub-aggregate attack launched by a few compromised nodes can inject arbitrary amount of error in the base station's estimate of the aggregate. We presented an attack-resilient computation algorithm which would guarantee the successful computation of the aggregate even in the presence of the attack.

REFERENCES

[1] A. Mishra, K. Nadkarni, A. Patcha, Intrusion detection in wireless Ad-hoc networks, IEEE Wirel. Commun. 11 (1) (2004) 48–60.

[2] Y. Zhang, W. Lee, Y.-A. Huang, Intrusion detection techniques for mobile wireless networks, Wirel. Netw. 9 (5) (2003) 545–556.

[3] M. La Polla, F. Martinelli, D. Sgandurra, A survey on security for mobile devices, IEEE Commun. Surv. Tutor. 15 (1) (2013) 446–471.

[4] F. Anjum, P. Mouchtaris, Intrusion Detection Systems, John Wiley & Sons, Inc., 2006.

[5] P. Brutch, C. Ko, Challenges in intrusion detection for wireless ad-hoc networks, in: Proceedings of Symposium on Applications and the Internet Workshops, 2003, pp. 368–373.

[6] Y.-C. Hu, A. Perrig, D. Johnson, Ariadne: a secure on-demand routing protocol for ad-hoc networks, Wirel. Netw. 11 (1–2) (2005) 21–38.

[7] S. Bu, F. Yu, X. Liu, P. Mason, H. Tang, Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks, IEEE Trans. Veh. Technol. 60 (3) (2011) 1025–1036.

[8] Z. Fadlullah, H. Nishiyama, N. Kato, M. Fouda, Intrusion detection system (IDS) for combating attacks against cognitive radio networks, IEEE Netw. 27 (3) (2013) 51–56.

[9] Y. Zhang, W. Lee, Intrusion detection in wireless ad-hoc networks, in: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, ACM, 2000, pp. 275–283.

[10] T. Anantvalee, J. Wu, A survey on intrusion detection in Mobile Ad Hoc Networks, in: Wireless Network Security, Signals and Communication Technology, Springer, 2007, pp. 159–180.

[11] A. Mitrokotsa, C. Dimitrakakis, Intrusion detection in MANET using classification algorithms: the effects of cost and model selection, Ad Hoc Netw. 11 (1) (2013) 226–237.

[12] C. Xenakis, C. Panos, I. Stavrakakis, A comparative evaluation of intrusion detection architectures for mobile ad hoc networks, Comput. Secur. 30 (1) (2011) 63–80.

[13] I. Butun, S. Morgera, R. Sankar, A survey of intrusion detection systems in wireless sensor networks, IEEE Commun. Surv. Tutor. 16 (1) (2014) 266–282.

[14] R. Mitchell, I. Chen, Effect of intrusion detection and response on reliability of cyber physical systems, IEEE Trans. Reliab. 62 (1) (2013) 199–210.

[15] A. Patel, M. Taghavi, K. Bakhtiyari, J.C. Jnior, An intrusion detection and prevention system in cloud computing: a systematic review, J. Netw. Comput. Appl. 36 (1) (2013) 25–41.

[16] M. Ficco, L. Romano, A generic intrusion detection and diagnoser system based on complex event processing, in: First International Conference on Data Compression, Communications and Processing, 2011, pp. 275–284.

[17] K. Liu, J. Deng, P.K. Varshney, K. Balakrishnan, An acknowledgment-based approach for the detection of routing misbehavior in MANETs, IEEE Trans. Mob. Comput. 6 (5) (2007) 536–550.

[18] E.M. Shakshuki, N. Kang, T.R. Sheltami, EAACK – a secure intrusion-detection system for MANETs, IEEE Trans. Ind. Electron. 60 (3) (2013) 1089–1098.

[19] Y. Liu, C. Comaniciu, H. Man, A Bayesian game approach for intrusion detection in wireless ad hoc networks, in: Proceedings of the 2006 Workshop on Game Theory for Communications and Networks, ACM, 2006.

[20] A. Agah, S. Das, K. Basu, M. Asadi, Intrusion detection in sensor networks: a non-cooperative game approach, in: Proceedings of Third IEEE International Symposium on Network Computing and Applications, 2004, pp. 343–346.

[21] T. Alpcan, T. Basar, A game theoretic approach to decision and analysis in network intrusion detection, in: Proceedings of 42nd IEEE Conference on Decision and Control, 2003, pp. 2595–2600.

[22] Y. Huang, W. Lee, A cooperative intrusion detection system for ad hoc networks, in: Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003, pp. 135–147.

[23] M. Kodialam, T. Lakshman, Detecting network intrusions via sampling: a game theoretic approach, in: Twenty-

Second Annual Joint Conference of the IEEE Computer and Communications, vol. 3, 2003, pp. 1880–1889.

[24] A. Mas-Colell, M. Whinston, J. Green, Microeconomic Theory, New York, Oxford University Press, 1995.

[25] T. Issariyakul, E. Hossain, Introduction to Network Simulator NS2, 1st ed., Springer Publishing Company, Incorporated, 2008.

[26] P. Barford, J. Kline, D. Plonka, A. Ron, A signal analysis of network traffic anomalies, in: Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement, 2002, pp. 71–82.

[27] A. Lakhina, M. Crovella, C. Diot, Mining anomalies using traffic feature distributions, Comput. Commun. Rev. 35 (4) (2005) 217–228.

[28] J. Dickerson, J. Dickerson, Fuzzy network profiling for intrusion detection, in: 19th International Conference of the North American Fuzzy Information Processing Society, 2000, pp. 301–306.

[29] A. Valdes, K. Skinner, Adaptive, model-based monitoring for cyber attack detection, in: Recent Advances in Intrusion Detection, vol. 1907, 2000, pp. 80– 93.

[30] M. Roesch, Snort – lightweight intrusion detection for networks, in: Proceedings of the 13th USENIX Conference on System Administration, 1999, pp. 229–238.

[31] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, et al., Specificationbased anomaly detection: a new approach for detecting network intrusions, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002, pp. 265–274.

[32] S. Marti, T.J. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, ACM, 2000, pp. 255– 265.

[33] S. Misra, P. Krishna, K. Abraham, Energy efficient learning solution for intrusion detection in Wireless Sensor Networks, in: Second International Conference on Communication Systems and Networks, 2010, pp. 1–6.

[34] F. Haddadi, M. Sarram, Wireless intrusion detection system using a lightweight agent, in: Second International Conference on Computer and Network Technology, 2010, pp. 84–87.

[35] M. Mohanapriya, I. Krishnamurthi, Modified DSR protocol for detection and removal of selective black hole attack in MANET, Comput. Electr. Eng. 40 (2) (2014) 530–538.