Security in Mobile Ad Hoc Networks

Pimal Khanpara and Bhushan Trivedi

Abstract Due to the proliferation of mobile devices, Mobile Ad hoc Networks (MANETs) are increasing in popularity. However, security of such networks is an important issue as MANETs are vulnerable to various attacks occurring at different layers of TCP/IP protocol suite. This paper focuses on the Network layer vulnerabilities as this layer is responsible for one of the basic MANET functions, routing. This paper describes the existing detection approaches for Network layer attacks. The comparison of the existing security solutions for Network layer attacks is also presented in this paper. Finally, the paper describes the scope of further research.

Keywords Mobile ad hoc networks · Security · Network layer · Point detection mechanisms · Intrusion detection schemes

1 Introduction

Mobile Ad hoc Networks are increasing in popularity but due to the basic characteristics of MANETs, they are vulnerable to various types of attacks. The operation of the network can be compromised by attacking at different layers of the network model. MANETs have many peculiar characteristics like limited battery and computational power, a lack of the centralized control entity, participation of

P. Khanpara (✉)
Institute of Technology, Nirma University, Ahmedabad, India
e-mail: pimal.khanpara@gmail.com

B. Trivedi
GLS Institute of Computer Technology, Ahmedabad, India
e-mail: bhtrivedi@gmail.com

© Springer Nature Singapore Pte Ltd. 2017

N. Modi et al. (eds.), *Proceedings of International Conference on Communication and Networks*, Advances in Intelligent Systems and Computing 508,
DOI 10.1007/978-981-10-2750-5_52

network nodes in the routing process, dynamic topology, mobility and short-term network services. Due to this, they are vulnerable to route level attacks. Unlike conventional networks, the job of routing is shouldered by the nodes themselves in MANETs and that introduces lot of additional issues. In this environment, conventional security measures like encryption and authentication fail to provide complete protection as conventional solutions are computation heavy and are not designed for battery limited and memory limited devices.

In the last few decades, many researchers have proposed large number of intrusion detection system prototypes for MANETs which are mainly classified into two categories: Point Detection Algorithms and Intrusion Detection Systems (IDSs). The following section presents a survey of Point Detection Algorithms and IDSs proposed in the literature to provide protection against network layer attacks in MANETs.

2 Network Layer Attacks

There are two main categories of Network Layer attacks in MANETs: Passive attacks and Active attacks. In passive attacks, the attacker does not try to affect the normal operation of the routing protocol but tries to get some valuable information about the network. Passive attacks in MANETs are categorized as: Eavesdropping, Traffic Analysis and Location Disclosure. In active attacks in MANETs, attackers try to disrupt the functioning of the network by altering, forging, dropping, fabricating or injecting data or control packets in the network. Active attacks are more severe compared to passive attacks as they can degrade the performance of the network significantly or bring down the network. Active attacks are mainly categorized as routing attacks, packet dropping attacks, Sleep Deprivation attacks, Black Hole attacks, Grey Hole attacks, Sybil attacks and Rushing attacks.

3 Point Detection Algorithms

This section presents a survey of different approaches proposed in the literature to defend from major network layer attacks. As shown in Fig. 1, protection mechanisms for Network Layer are classified based on the number of attacks they can detect. Point detection algorithms can detect only a single type of attack at Network Layer. The other category, intrusion detection systems can identify a range of attacks. Point detection algorithms are further divided according to the type of attack they detect. Table 1 shows the analysis of existing point detection mechanisms for network layer attacks.

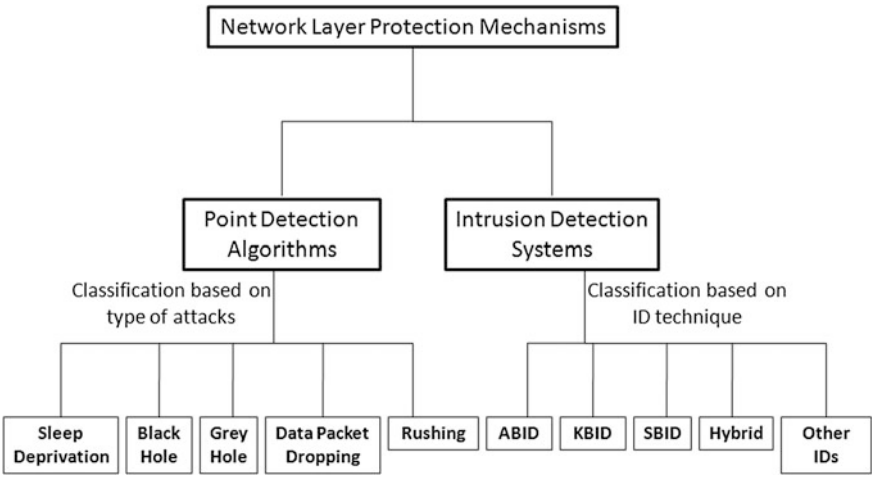

Fig. 1 Network layer protection mechanisms

4 Intrusion Detection Algorithms

Intrusion Detection Systems (IDSs) can detect a range of attacks. This section reviews the existing IDSs and challenges faced by them in MANETs. There are three main categories of IDSs: Knowledge Based Intrusion Detection Systems (KBIDs), Anomaly Based Intrusion Detection Systems (ABIDs), Specification Based Intrusion Detection Systems (SBIDs). In MANETs, some IDSs are combinations of two or more types of intrusion detection techniques and are known as Hybrid Intrusion Detection Systems.

KBIDSs are also known as misuse detection systems. They use and maintain a knowledge base consisting of patterns or signatures of well-known attacks. They add new rules in the knowledge base for unknown attacks. Compared to other IDSs, KBIDSs have very low false positive rates of detection. The limitation of KBIDSs is that they are able to detect only those attacks whose signatures or patterns are available in the knowledge base. Moreover, it is tedious to keep the knowledge base up-to-date for maintaining information about attacks.

ABIDs are also known as behavior based IDSs. They observe the anomalous activities to detect the intrusion and work in two phases: Training Phase and Testing Phase. Training phase is used to model the normal expected behavior of the network. Testing phase compares the current behavior model of the network with the expected behavior model. The main advantage of these systems is that they try to exploit unknown attacks. The drawback of ABIDs is that they are prone to generate false alarms.

SBIDs use explicitly defined specifications to monitor the operations performed at the network layer. Initially, they extract the specifications that specify the correct functionality of the network. In the next step, the system monitors the execution of

Table 1 Point detection algorithms

Protocol name	Architecture	Attacks detected	Detection technique	Corrective measures	Routing protocol	Data gathering mechanism	Remarks
FAP (Yi et al. [1])	Distributed	Sleep deprivation caused by malicious route requests	Priority queue of route requests	Exclude attackers	AODV	Single node monitoring	May suppress legitimate nodes
None (Martin et al. [2])	Not specified	Sleep deprivation	Energy signature, multilevel authentication	Not specified	Not specified	Requests to SSH server	Analyzes the effect of sleep deprivation attack on real systems
LIP (Hsu et al. [3])	Not specified	Sleep deprivation	Local broadcast authentication	Not specified	Not specified	Observation by nodes	Lightweight; helps to prevent packet injection and impersonation
None (Sarkar and Roy [4])	Hierarchical	Sleep deprivation	Based on cluster head's decision	Not specified	Not specified	Observation of packet forwarding	It is not specified how to determine threshold value for packet forwarding
TOGBAD (Pedillia et al. [5])	Centralized, hierarchical	Black hole	Topology graph	Not specified	OLSR	Topology graph	Not feasible for reactive routing
None (Medadian et al. [6])	Distributed	Black hole	Finding safe path	Not specified	AODV	Neighbors' observation	May generate false alarm in highly dynamic MANETs
None (Zhang et al. [7])	Distributed	Black hole	Verifying sequence number of route reply	Not specified	AODV, SAODV	Intermediate nodes' observation	Increased overhead, lack of security checks for sequence request and reply packets

(continued)

Table 1 (continued)

Protocol name	Architecture	Attacks detected	Detection technique	Corrective measures	Routing protocol	Data gathering mechanism	Remarks
None (Xiaopeng et al. [8])	Distributed	Grey hole	Checkup, proof and diagnosis algorithms	Not specified	DSR	Proof from forwarded packets	Specific to DSR
None (Wei et al. [9])	Distributed	Grey hole	Aggregate signature algorithm	Not specified	Not specified	Aggregate signature algorithm	A certificate authority is assumed to be present
None (Yang et al. [10])	Not specified	Grey hole	Historical evidence	Not specified	Not specified	Neighbors' observation	Historical trust values are used to make detection decision
None (Sharma and Garg [11])	Not specified	Sybil	Considered RSS, node speed	Not specified	Not specified	Node speed observation	Threshold value of speed is 10 m/s
None (Abbas et al. [12])	Not specified	Sybil	Localization process	Not specified	Not specified	Localization process	Once a node is registered, no further localization is performed
None (Tangpong et al. [13])	Not specified	Sybil	Exchanging observed information	Exclude attackers	Not specified	Cooperative monitoring	No central authority is needed
None (Hashmi and Brooke [14])	Not specified	Sybil	Authentication agent	Not specified	Not specified	Verification by authentication agent	Uses hardware id for authentication
RAP (Hu et al. [15])	Distributed	Rushing attack	Mutual authentication protocol	Not specified	DSR	Neighbors' observation	Specific to DSR
SRP (Papadimitratos and Haas [16])	Not specified	Rushing attack	SMT protocol	Not specified	Not specified	SMT protocol	Effectiveness of SRP is not checked against routing attacks in MANETs

(continued)

Table 1 (continued)

Protocol name	Architecture	Attacks detected	Detection technique	Corrective measures	Routing protocol	Data gathering mechanism	Remarks
None (Gonzalez et al. [17])	Distributed	Packet dropping	Adaptive policies	Not specified	Not specified	Distributed management overlay	Adaptable protection of routing protocols
SCAN (Yang et al. [18])	Distributed	Packet dropping	Information cross validation	Exclude attackers	AODV	Collaborative monitoring	Specific to reactive routing process
None (Shu and Krunz [19])	Not specified	Packet dropping	Correlation between lost packets	Not specified	Not specified	Public auditing architecture	Increased overhead

Table 2 IDS Algorithms

Algorithm name	Architecture	Attacks detected	Intrusion detection technique	Corrective measures	Routing protocol	Data gathering mechanism	Remarks
None (Liu et al. [20])	Distributed	DoS	Bayesian game theory based anomaly detection	Not specified	Not specified	Lightweight and heavyweight monitoring systems	Use of two IDS
None (Sun et al. [21])	Distributed	Routing disruption attacks	Anomaly detection using Markov chain classifier	Not specified	Not specified	Audit data sources	Can detect local intrusion
None (Jabbehdari et al. [22]	Not specified	DoS	Anomaly detection using neural networks	Not specified	Not specified	Trace output	Specific to DoS attacks
AIDP (Nadeem and Howarth, [23])	Clustered, hierarchical	DoS	Anomaly detection	Exclude intruders	General; tested on AODV	Routing information	Specific to DoS attacks
AFIDS (Chaudhary et al. [24])	Not specified	Black hole	Fuzzy based anomaly detection	Exclude intruders	AODV	Network monitoring	Performance depends on the accuracy of fuzzy inference engine
None (Komninos et al. [25])	Not specified	Not specified	Knowledge based detection	Not considered	Not specified	Audit data trails	Not tested against attacks
IDAR (Alattar et al. [26])	Distributed	Pattern matching	Signature based detection	Not specified	OLSR	Logs generated by OLSR	High bandwidth and memory requirement

(continued)

Table 2 (continued)

Algorithm name	Architecture	Attacks detected	Intrusion detection technique	Corrective measures	Routing protocol	Data gathering mechanism	Remarks
AODVSTAT (Vigna et al. [27])	Distributed	Resource depletion, packet dropping	Knowledge based detection	Not specified	AODV	AODV routing packets, data packets	Detects the attacks against AODV only
None (Tseng et al. [28])	Distributed	DoS	FSM based SBID	Not specified	OLSR	OLSR information	Specific to OLSR
EFSM (Orset et al. [29])	Distributed	Sybil, modification, fabrication	Extended FSM based SBID	Not specified	OLSR	OLSR information	Specific to OLSR protocol
None (Stakhanova et al. [30])	Not specified	Behavioral specification	Specification based detection	Not specified	AODV, DSR	Network traffic flow	Specific to AODV and DSR
CRADS (Joseph et al. [31])	Not specified	Rushing, medication, spoofing, packet dropping	Hybrid intrusion detection	Not specified	OLSR	Data collected from physical, MAC, network layer	Cross layer approach
GIDP (Nadeem and Howarth [32])	Clustered, hierarchical	Various network layer attacks	Hybrid intrusion detection	Exclude attackers	General	Network characteristics; performance matrix	Tested using AODV
None (Yi et al. [33])	Clustered, hierarchical	Routing loops, DoS	Other IDS	Generate alarm	DSR	DSR specifications	Specific to DSR

the operations with respect to the given specification. If it finds any deviation from the specification then it detects it as intrusion.

Table 2 shows the analysis of various intrusion detection systems proposed in the literature.

5 Conclusion

The existing intrusion detection techniques for Mobile Ad hoc Networks are categorized as either Point detection or Intrusion detection schemes. They focus on specific attacks, capable of detecting one or multiple attacks. Many existing reactive security mechanism for MANETs are studied in this paper. From their comparison, we can say that none of these schemes are able to defend against all possible attacks. Moreover, most of the schemes also add additional overhead and complexity in the normal functioning of the network. Hence, there is scope to propose a new security solution for MANETs that is robust and lightweight.

References

1. Yi, P., Dai, Z., Zhong, Y., Zhang, S.: Resisting Flooding Attack in Ad Hoc Networks. In: IEEE International Conference on Information Technology Coding & Computing, pp. 657–662 (2005).
2. Martin, T., Hsiao, M, Dong, H., Krishnaswami, J.: Denial-of-Service Attacks on Battery Powered Mobile Computers. In: IEEE International Conference on Pervasive Computing and Communications (PerCom) (2004).
3. Hsu, H., Zhu, S., Hurson, A. R.: LIP—a Lightweight Interlayer Protocol for Preventing Packet Injection Attacks in Mobile Ad Hoc Networks. In: International Journal of Security and Networks, Vol. 2, Nos. 3/4, pp. 202–215 (2007).
4. Sarkar, M., Roy D. B.: Prevention of Sleep Deprivation Attacks using Clustering. In: IEEE ICECT, Vol. 5, pp. 391–394 (2011).
5. Padilla, E., Aschenbruck, N., Martini, P., Jahnke, M., Tolle J.: Detecting Black Hole Attack in Tactical MANETs using Topology Graph. In: IEEE Conference on Local Computer Networks (2007).
6. Medadian M., Yektaie M. H., Rehmani, A. M.: Combat with Black Hole Attack in AODV Routing Protocol in MANETs. In: IEEE Asian Himalayas International Conference on Internet (2009).
7. Zhang, X. Y., Sekiya Y., Wakahara, Y.: Proposal of a Method to Detect Black Hole Attack in MANETs. In: IEEE International Symposium on Autonomous Decentralized System ISADS (2009).
8. Xiaopeng, G., Wei, C.: A Novel Grey Hole Attack Detection Scheme for Mobile Ad-Hoc Networks. In: IFIP International Conference on Network and Parallel Computing (2007).
9. Wei, C., Xiang, L., Yuebinand, B., Xiopeng, G.: A New Solution for Resisting Grey Hole Attack in Mobile Ad Hoc Networks. In: IEEE Conference on Communication and Networking, China (2007).
10. Yang, B., Yamamoto, R., Tanaka, Y.: Historical Evidence Based Trust Management Strategy against Black Hole Attacks in MANET. In: IEEE ICACT, pp. 394–399 (2012).

11. Sharma, H., Garg, R.: Enhanced Lightweight Sybil Attack Detection Technique. In: IEEE Confluence, pp. 476–481 (2014).
12. Abbas, S., Merabti, M., Jones, D.: Signal Strength Based Sybil Attack Detection in Wireless Ad hoc Networks. In: IEEE DESE, pp. 190–195 (2009).
13. Tangpong, A., Kesidis, G., Hsu, H., Hurson, A.: Robust Sybil Detection for MANETs, In: IEEE ICCCN, pp. 1–6 (2009).
14. Hashmi, S., Brooke, J.: Towards Sybil Resistant Authentication in Mobile Ad hoc Networks. In: IEEE Secureware, pp. 17–24 (2010).
15. Hu, Y., Perrig, A., Johnson, B.: Rushing Attack and Defence in Wireless Ad Hoc Networks Routing Protocol. In: ACM Workshop on Wireless Security, pp. 30–40 (2003).
16. Papadimitratos, P., Haas, Z. J.: Secure Message Transmission in Mobile Ad Hoc Networks. In: Elsevier Journal of Ad Hoc Networks, Vol. 1, No. 1, pp. 193–209 (2003).
17. Gonzalez-Duque, O. F., Hadjiantonis, A. M., Pavlou, G., Howarth, M.: Adaptive Misbehaviour Detection and Isolation in Wireless Ad Hoc networks Using Policies. In: IFIP/IEEE International Symposium on Integrated Network Management, pp. 242–250, NY, USA (2009).
18. Yang, H., Shu, J., Meng, X., Lu, S.: SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks. In: IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 261–273 (2006).
19. Shu, T., Krunz, M.: Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks. In: IEEE Transactions on Mobile Computing, Vol. 14, issue 4, pp. 813–828 (2014).
20. Liu, Y., Comaniciu, C., Man, H.: Modelling Misbehaviour in Ad Hoc Networks: a Game Theoretic Approach for Intrusion Detection. In: International Journal of Security and Networks, Vol. 1, Nos. 3/4, pp. 243–254 (2006).
21. Sun, B., Wu, K., Xiao, Y., Wang, R.: Integration of Mobility and Intrusion Detection Wireless Ad Hoc Networks. In: Journal of Communication Systems, Wiley International, Vol. 20, No. 6, pp. 695–721 (2007).
22. Jabbehdari, S., Talari, S. H., Modiri, N.: A Neural Network Scheme for Anomaly Based Intrusion Detection Systems in Mobile Ad Hoc Networks. In: Journal of Computing, Vol. 4, No. 2, pp. 61–66 (2012).
23. Nadeem, A., Howarth, M.: Adaptive Intrusion Detection & Prevention of Denial of Service Attacks in MANETs. In: ACM International Wireless Communication and Mobile Computing Conference, Leipzig Germany (2009).
24. Chaudhary, A., Tiwari, V., Kumar, A.: Design an Anomaly Based Fuzzy Intrusion Detection System for Packet Dropping Attack in Mobile Ad Hoc Networks. In: Proceedings of IEEE IACC, pp. 256–261 (2014).
25. Komninos, N., Vergados, D., Douligeris, C.: Detecting Unauthorized and Compromised Nodes in Mobile Ad Hoc Networks. In: Journal of Ad Hoc Networks, Elsevier, Vol. 5, No. 3, pp. 289–298 (2007).
26. Alattar, M., Sailhan, F., Bourgeois, J.: Log-based Intrusion Detection for MANET. In: Proceedings of IEEE IWCMC, pp. 697–702 (2012).
27. Vgina, G., Gawalani, S., Srinivasan, K., Belding-Royer, M., Kemmerer, A: An Intrusion Detection Tool for AODV Based Ad Hoc Wireless Networks. In: IEEE Annual Computer Security Application Conference ACSAC (2004).
28. Tseng, H., Song, T., Balasubramanyam, P., Ko, C., Levitt, K.: A Specification-Based Intrusion Detection Model for OLSR. In: International Symposium on Recent Advances in Intrusion Detection (RAID), pp. 330–350 (2005).
29. Orset, J. M., Alcalde, B., Cavalli, A. R.: An eEFSM-Based Intrusion Detection System for Ad Hoc Networks. In: International Conference on Automated Technology for Verification and Analysis, pp. 400–413 (2005).
30. Stakhanova, N., Basu, S., Zhang, W., Wang, X., Wong, J.: Specification Synthesis for Monitoring and Analysis of MANET Protocols. In: International Symposium on Frontiers in Networking with Applications (2007).

31. Joseph, J., Das, A., Seet, B., Lee, B.: CRADS: Integrated Cross Layer approach for Detecting Routing Attacks in MANETs. In: IEEE Wireless Communication and Networking Conference (WCNC) (2008).
32. Nadeem, A., Howarth, M.: A Generalized Intrusion Detection and Prevention Mechanism for Securing MANETs. In: IEEE International Conference on Ultra Modern Telecommunications and Workshops, St Petersburg Russia (2009).
33. Yi, P., Jiang, Y., Zhong, Y., Zhang, S.: Distributed Intrusion Detection for Mobile Ad Hoc Networks. In: IEEE Application and Internet Workshop (2005).