An Effective Double Acknowldgement Scheme for Intrusion Detection in Mobile Ad Hoc Networks

Dickson Leon I [1] V. Hari Prasanth [2] S. Kiruthika[3] (AP)
Department Of ECE KPR
Institute of Engineering and Tech

Abstract:**The hegira to wireless network from wired network has been a worldwide trend in the past few years. The mobility and scalability brought by a wireless network made it possible in many application. Mobile Ad Hoc Network (MANET) is one of the most predominant and idiosyncratic applications. On the contrary to accustomed network architecture, MANET does not require a fixed network infrastructure, every single node works as Transceiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise , they reckon on their neighbours to relay messages. The Self-configuring ability of nodes in MANET made it popular among critical mission application like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET impuissant to rancorous attackers. In this case, it is pivotal to develop efficient encroachment-detection mechanisms to protect MANET from attacks. To adjust to such trend , we strongly believe that it is vital to address its potential security issues. In this paper, we propose and implement a new encroachment-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETSs . Compared to coeval approaches, EAACK demonstrates higher rancorous behaviour-detection ratesin certain circumsatances while does not greatly affect the network performances**

Keywords- Eaack ,manet ,rancorous attacks, relay messages.

1.INTRODUCTION

Due to their natural mobility and scalability, wireless networks are always preferred since the first day of their invention. Owing to the improved technology and reduced costs, wireless networks have gained much more preferences over wired networks in the past few decades. Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly.Industrial remote access and control via wireless networks are becoming more and more popular these days [1]. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly [1], [2], [3]. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations [4], [5].

The unique characteristics of MANET is becoming more and more widely implemented in the industry [5],[6]. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection,malicious attackers can easily capture and compromise nodes to achieve attacks.

1.1 MANETs Detection System:

Due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, an IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches [10]. Anantvalee and Wu presented a very thorough survey on contemporary IDSs in MANETs.

1.2 OLD Version System:

In this section, we mainly describe three existing approaches, namely, Watchdog [7], TWOACK [8], andAdaptive ACKnowledgment (AACK) [9].

1.2.1 Improvisation of Rancorous in IDS:

Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater.Watchdog serves as an IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network.Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmissionThese advantages have made the Watchdog scheme a popular choice in the field. The Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions;3) limited transmission power; 4) false misbehavior report;5) collusion; and 6) partial dropping.

1.2.2 To Overcome The Disadvantage Of WATCHDOG:

With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu *et al.* [8] is one of the most important approaches among them. On Fig. 1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it. the contrary to many other schemes, TWOACK is neither an enhancement nor aWatchdog-based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR) [11].

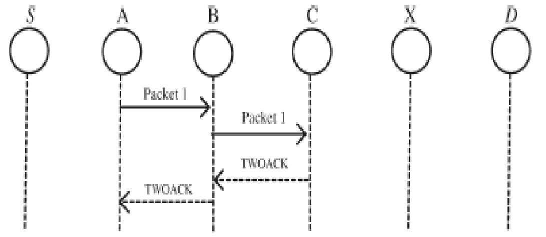

Fig. 1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

1.2.3Advantage Version Of TWO ACK (AACK):

Based on TWOACK, Sheltami *et al.* [14] proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. The end-to-end acknowledgment scheme in ACK is shown in Fig. 2. In the ACK scheme shown in Fig. 2, the source node S sends out Packet 1 without any overhead except 2 b of flag indicating the packet type. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of thesame route.

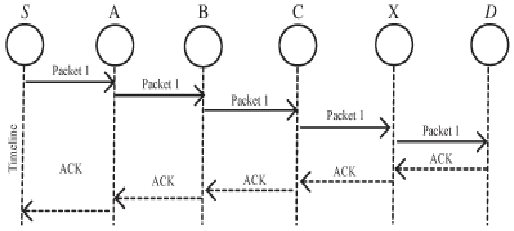

Fig. 2. ACK scheme: The destination node is required to send acknowledgment packets to the source node.

1.2 *EAACK$_S$ Error Detection:*

Our proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision.In this section, we discuss these three weaknesses in detail. In a typical example of receiver collisions, shown in Fig. 4, after node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding Packet 2 to node C. In such case, node A overhears that node B has successfully forwarded Packet 1 to node C but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.In the case of limited transmission power, in order to preserve its own battery resources, node B intentionally limits its transmission power so that it is strong enough to be overheard by node A but not strong enough to be received by node C, as shown in Fig. 5. As discussed in previous sections, TWOACK and AACK solve two of these three weaknesses, namely, receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehavior attack. In this research work, our goal is to propose a new IDS specially designed for MANETs, which solves not only receiver collision and limited transmission power but also the false misbehavior problem. Furthermore, we extend our research to adopt a digital signature scheme during the packet transmission process. As in all acknowledgment-based IDSs, it is vital to ensure the integrity and authenticity of all acknowledgment packets.

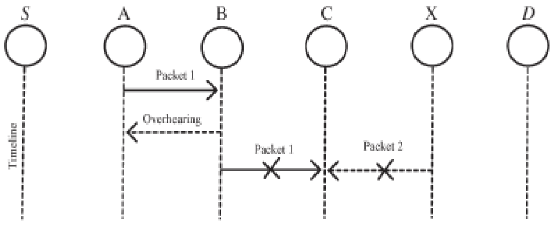

Fig. 4. Receiver collisions: Both nodes B and X are trying to send Packet 1 and Packet 2, respectively, to node C at the same time.

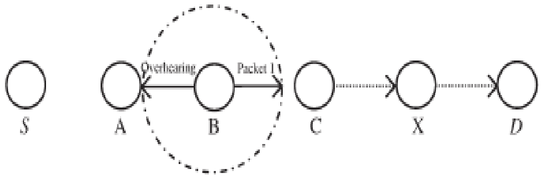

Fig. 5. Limited transmission power: Node B limits its transmission power so that the packet transmission can be overheard by node A but too weak to reach node C.

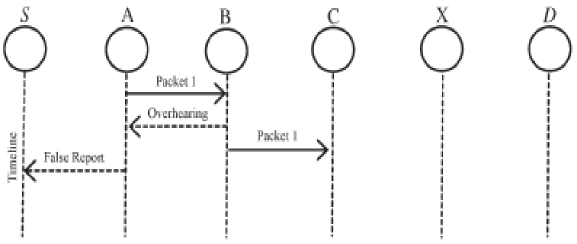

Fig. 6. False misbehavior report: Node A sends back a misbehavior report even though node B forwarded the packet to node C.

1.4 Proposed Scheme

Many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. To address this concern, we adopt a digital signature in our proposed scheme named Enhanced AACK (EAACK).

EAACK is consisted of three major parts, namely, ACK,secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes, we included a 2-b packet header in EAACK. According to the Internet draft of DSR [11], there is 6 breserved in the DSR header. In EAACK, we use 2 b of the 6 b to flag different types of packets. Details are listed in Table I. Fig. 7 (shown later) presents a flowchart describing the EAACK scheme. Please note that, in our proposed scheme, we assume that the link between each node in the network is bidirectional. Furthermore, for each communication process, both the source node and the destination node are not malicious.

1.4.1 ACK

As discussed before, ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In Fig. 8, in ACK mode, node S first sends out an ACK data packet *Pad*1 to the destination node D.If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives *Pad*1, node D is required to send back an ACK acknowledgment packet *Pak*1 along the same route but in a reverse order. Within a predefined time period, if node S receives *Pak*1, then the packet transmission from node S to node D is successful.

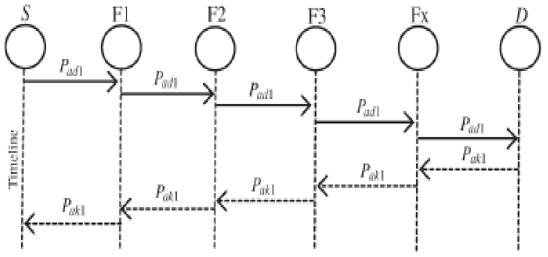

Fig. 7. System control flow: This figure shows the system flow of how the EAACK scheme works.

1.4.2 MRA

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehaviour report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes.By adopting an alternative route to the destination node, we circumvent the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted.By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehaviour report.

1.4.3 Digital Signature

As discussed before, EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted.Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable.

2.PERFORMANCE EVALUATION

In this section, we concentrate on describing our simulation environment and methodology as well as comparing performances through simulation result comparison with Watchdog, TWOACK, and EAACK schemes.

2.1 Simulation Methodologies

To better investigate the performance of EAACK under different types of attacks, we propose three scenario settings to simulate different types of misbehaviors or attacks.

Scenario 1: In this scenario, we simulated a basic packet dropping attack. Malicious nodes simply drop all the packets that they receive. The purpose of this scenario is to test the performance of IDSs against two weaknesses of Watchdog, namely, receiver collision and limited transmission power.

Scenario 2:
This scenario is designed to test IDSs' performances against false misbehavior report. In this case, malicious nodes always drop the packets that they receive and send back a false misbehavior report whenever it is possible.

2.2 Simulation Configuration

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with GCC 4.3 and Ubuntu 9.10. The system is running on a laptop with Core 2 Duo T7250 CPU and 3-GB RAM. In order to better compare our simulation results with other research works, we adopted the default scenario settings in NS2.34. The intention is to provide more general results and make it easier for us to compare the results. In NS 2.34, the default configuration specifies 50 nodes in a flat space with a size of 670 × 670 m. The maximum hops allowed in this configuration setting are four. Both the physical layer and the
802.11 MAC layer are included in the wireless extension of NS2. The moving speed of mobile node is limited to 20 m/s and a pause time of 1000 s. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512 B. For each scheme, we ran every network scenario three times and calculated the average performance.

2.2.1 Packet delivery ratio (PDR):

PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

2.2.2Routing overhead (RO):

RO defines the ratio of the amount of routing-related transmissions [Route REQuest(RREQ), Route REPly (RREP), Route ERRor (RERR),ACK, S-ACK, and MRA].

2.3 Performance Evaluation

To provide readers with a better insight on our simulation results, detailed simulation data are presented in Table II.

2.3.1 Simulation Results

Scenario 1: In scenario 1, malicious nodes drop all the packets that pass through it. Fig. 10 shows the simulation results that are based on PDR.In Fig. 10, we observe that all acknowledgment-based IDSs perform better than the Watchdog scheme. Our proposed scheme EAACK surpassed Watchdog's performance by 21% when there are 20% of malicious nodes in the network. From the results, we conclude that acknowledgment-based schemes, including TWOACK, AACK, and EAACK, are able to detect misbehaviors with the presence of receiver collision and limited transmission power. However, when the number of malicious nodes reaches 40%, our proposed scheme EAACK's performance is lower than those of TWOACK and AACK. We generalize it as a result of the introduction of MRA scheme, when it takes too long to receive an MRA acknowledgment from the destination node that the waiting time exceeds the predefined threshold.

Scenario 2*:* In the second scenario,we set all malicious nodes to send out false misbehavior report to the source node whenever it is possible. This scenario setting is designed to test the IDS's performance under the false misbehavior report.

The achieved simulation results based on PDR. When malicious nodes are 10%, EAAC performs 2% better than AACK and TWOACK. When the malicious nodes are at 20% and 30%,

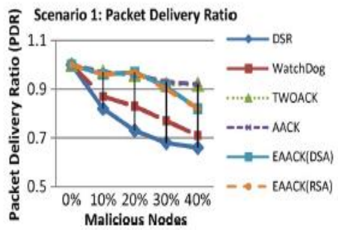

Fig. 10. Simulation results for scenario 1—PDR.

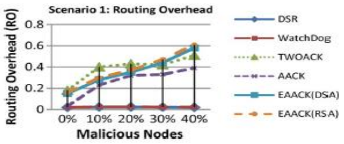

Fig. 11. Simulation results for scenario 1—RO.

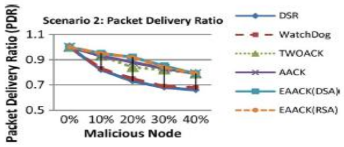

Fig. 12. Simulation results for scenario 2—PDR.

When the malicious nodes are at 20% and 30%,

EAACK outperforms all the other schemes and maintains the PDR to over 90%. We believe that the introduction of MRA scheme mainly contributes to this performance. EAACK is the only scheme that is capable of detecting false misbehavior report. In terms of RO, owing to the hybrid scheme, EAACK maintains a lower network overhead compared to TWOACK in most cases. However, RO rises rapidly with the increase of malicious nodes. Simulation results for scenario 3—RO. malicious nodes require a lot more acknowledgment packets and digital signatures.

2.4 DSA and RSA:

In all of the three scenarios, we witness that the DSA scheme always produces slightly less network overhead than RSA does. This is easy to understand because the signature size of DSA is much smaller than the signature size of RSA. However, it is interesting to observe that the RO differences between RSA and DSA schemes vary with different numbers of malicious nodes. The more malicious nodes there are, the more ROs the RSA scheme produces. We assume that this is due to the fact that more malicious nodes require more acknowledgment packets, thus increasing the ratio of digital signature in the whole network overhead. With respect to this result, we find DSA as a more desirable digital signature scheme in MANETs. The reason is that datatransmission in MANETs consumes the most battery power.

3.CONCLUSION

Packet-dropping attack has always been a major threat to the security in MANETs. In this research paper, we have proposed a novel IDS named EAACK protocol specially designed for MANETs and compared it gainst other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. . Although it generates more ROs in some cases, as demonstrated in our experiment, it can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets.We think that this tradeoff is worthwhile when network security is the top priority. In order to seek the optimal DSAs in MANETs, we implemented both DSA and RSA schemes in our simulation. Eventually, we arrived to the conclusion that the DSA scheme is more

suitable to be implemented in MANETs.To increase the merits of our research work, we plan to
investigate the following issues in our future research:

3.1 Future Work :

1) possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature;
2) examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of predistributed keys;
3) testing the performance of EAACK in real network environment instead of software simulation.

REFERENCES

[1] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," *IEEE Trans. Ind. Electron.*,
vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[2] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in *Lecture Notes in Electrical Engineering*, vol. 127.New York: Springer-Verlag, 2012, pp. 659–666.

[3] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana, India, 2012, pp. 535–541.

[4] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in *Wireless/Mobile Security*. New York: Springer-Verlag, 2008.

[5] L. Buttyan and J. P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 7,pp. 2759–2766, Jul. 2008.

[7] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks:Challenges, design principles, and technical approach," *IEEE Trans. Ind.Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[8] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl.*, 2002, pp. 3–13.

[9] Y. Hu, A. Perrig, and D. Johnson, “ARIADNE: A secure on-demand routing protocol for ad hoc networks,” in *Proc. 8th ACM Int. Conf. MobiCom*, Atlanta, GA, 2002, pp. 12–23.

[10] G. Jayakumar and G. Gopinath, “*Ad hoc* mobile wireless networks routing protocol—A review,” *J. Comput. Sci.*, vol. 3, no. 8, pp. 574–582,2007.