IPHV7I20029X

International Journal Of Advanced Research and Innovation -Vol.7, Issue .II

ISSN Online: 2319 – 9253

Print: 2319 – 9245

EAACK-NEW INTRUSION DETECTION SYSTEM FOR MOBILE SECURITY ISSUES

#1 A.Vijetha - M.Tech Pursuing,
#2 Dr. B. Sasidhar - Professor,
Department of Computer Science & Engineering,
MAHAVEER INSTITUTE OF SCIENCE & TECHNOLOGY, Hyderabad.

Abstract- Mobile Ad hoc networks (MANETs) consist of a set of mobile nodes which can move about freely. Due to the self configuring ability of nodes and its infrastructure less nature, MANETs are preferred in significant applications. This itself emphasizes the importance of security and the need for an efficient intrusion detection system in MANETs. Many IDS have been proposed for detecting malicious nodes. On such IDS, Enhanced Adaptive Acknowledgment (EAACK) has overcome the drawbacks of Watchdog, ACK and TwoACK. In our paper, we have identified the inadequate nature of EAACK in scenarios of link breakage, source maliciousness and partial packet dropping and hence we propose an improved algorithm called improved EAACK to tackle the security issues. High mobility of MANET nodes contributes to frequent link breakages in the network which leads to path failures and route discovery processes. Route discovery is initialized through broadcast mechanism usually. But, the overheads created through this cannot be neglected. Hence, in addition to security, reducing routing overhead is another criterion that is focused in order to improve the network performance that includes packet delivery ratio enhancement and delay reduction. Thus, the improved EAACK of ours successfully detects malicious nodes during link breakage, source maliciousness, identifies partial packet droppers, overcomes receiver collision, tackled limited transmission problems and identifies forged acknowledgments and false misbehavior report.

Keywords- Mobile Ad hoc networks (MANET), Intrusion detection system (IDS), EAACK, improved EAACK, AODV, RSA, partial packet dropping, iterative classification.

I. INTRODUCTION

MANET (Mobile Ad hoc network) is an IEEE 802.11 framework which is a collection of mobile nodes equipped with both a wireless transmitter and receiver communicating via each other using bidirectional wireless links. This type of peer to peer system infers that each node or user in the network can act as a data endpoint or intermediate repeater. Thus, all users work together to improve the reliability of network communications. MANETs are self-forming, self-maintained and self-healing allowing for extreme network flexibility, which is often used in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances.

MANETs are an appealing technology for many applications such as rescue and tactical operations due to the flexibility provided by their infrastructure. However, this flexibility comes at a price and introduces new security threats. Furthermore, many conventional security solutions used are ineffective and inefficient for the highly dynamic and resource constrained environments where MANETs use might be expected. Unfortunately, the remote distribution and open medium of MANET makes them susceptible to various attacks. For example, due to lack of protection for nodes, malicious attackers can easily capture and compromise the mobile nodes to achieve attacks. Particularly, considering the fact – that most routing protocols in MANETs assume that every node in the network behave cooperatively with other nodes and presumably not a malicious one; attackers can easily compromise MANETs by inserting malicious or non-cooperative node into the network. Due to MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. Hence, it is crucial to develop an intrusion detection system in MANETs. In this paper, we aim to develop such an efficient and reliable intrusion detection system (IDS).

II. BACKGROUND

With the upgrading technology, we are witnessing the expansion of MANETs into industrial application. So it is vital to address its security issues. Such existing IDSs in MANETs are 1) Watchdog 2) TWOACK and 3) AACK.

1. Watchdog

Watchdog improves the throughput of the network even in the presence of attackers. It has two parts namely Watchdog and Path rater. It detects malicious nodes by overhearing next hop's transmission. A failure counter is initiated if the next node fails to forward the data packet. When the counter value exceeds a predefined threshold, the node is marked malicious. The major drawbacks are 1) ambiguous collisions 2) receiver collisions 3) limited transmission power 4) false misbehavior report 5) partial dropping 6) collusion.

2. TWOACK

TWOACK overcomes the receiver collision and limited transmitted power limitation of Watchdog. Here acknowledgment of every data packet over every three consecutive nodes is sent from source to destination. If ACK is not received in a predefined time, the other two nodes are marked malicious. The major drawbacks are 1) Increased overhead 2) Limited battery power 3) Degrades the life span of entire network.

3. AACK

Adaptive acknowledgement is the combination of TWOACK and ACK. Source sends packet to every node till it reaches the destination. Once reached, receiver sends an ACK in the reverse order. If ACK is not received within predefined interval, it switches to TWOACK scheme. The major drawbacks is that it suffers from 1) False misbehavior report2) Forged acknowledgment packets.

Digital signature

Digital signature is a widely adopted approach to ensure the authentication, integrity, and no repudiation of MANETs. All algorithms except watchdog are based on acknowledgment. Hence, it should be authenticated through digital signature.

EAACK

Enhanced Adaptive ACKnowledgment is designed to tackle false misbehavior, limited transmission power and receiver collision limitations of watchdog. It involves three parts namely ACK, SACK (Secure ACK), MRA (misbehavior report authentication). Digital signature is used in EAACK to prevent the nodes from forged acknowledgement attacks. This scheme is explained in detail later.

III. LITERATURE REVIEW

N. Kang, E. Shakshuki and T. Sheltami proposed a scheme called Enhanced Adaptive ACKnowledgement (EAACK). This scheme aims to overcome four of the weaknesses in traditional Watchdog mechanism, namely, ambiguous collisions, receiver collisions, limited transmission power and false misbehavior. But there is no authentication for acknowledgements. The functions of detection scheme largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. So this scheme is not much efficient. Although the simulation result showed that the proposed scheme outputs higher packet delivery ratio, it also has a higher overhead ratio with the increase of malicious nodes in the network. This is due to the introduction of MRA scheme. Elhadi M. Shakshuki proposed EAACK which was designed with the implementation of RSA and DSA digital signatures using DSR routing protocol. Performance evaluation was done and results were obtained. But this EAACK has no provision for handling link breakage and malicious source node scenario. Later the introduction of digital signature to prevent the attacker from forging acknowledgment packets was proposed. It used a new protocol for better security using hybrid cryptographic technique to reduce the overhead caused by digital signature. But it had no provision for handling link breakage and malicious source node scenario. Thus all the existing IDSs have certain disadvantages.

IV. EAACK

In the existing approach, EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely false misbehavior, limited transmission power and Receiver collision. EAACK consists of three major parts, ACK, Secure ACK (S-ACK) and misbehavior report authentication (MRA).

A. ACK

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.

B. S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

C. 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 misbehavior 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.

D. Digital Signature

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. With regard to this urgent concern, digital signature scheme has been incorporated into EAACK. Hence, we have authenticated all the acknowledgments using RSA algorithm.

We, analyzed the performance of existing EAACK in various scenarios and found that it gave poor performance during

A. Scenario 1: Link breakage, occurs due to
- Continuously changing network topology
- High mobility of nodes
- Factors like traffic and delay
- Nodes move beyond transmission range
- Insufficient energy levels

B. Scenario 2: Malicious source node, resulting in
- Packet drop
- Drained battery • Buffer overflow
- Message tampering • Fake routing
- Stealing information.

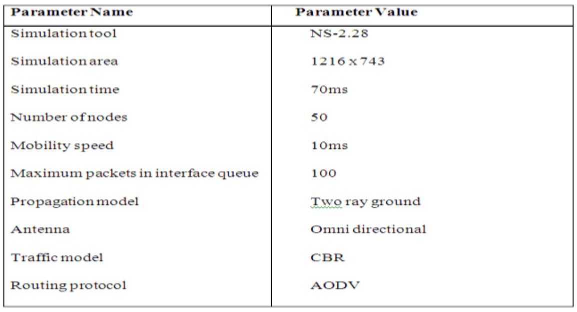
C. Partial packet dropping
D. Resulting in Increased routing overhead, delay
E. Reduced packet delivery ratio.

V. SIMULATION WORK

A. SIMULATION CONFIGURATION

Our simulation is carried out within the Network Simulator 2.28 in Windows Xp operating system with Cygwin as the interface tool. There are 50 nodes defined in a simulation area of size 1216 x 74. The mobility of nodes is limited to 10ms. The traffic model chosen is Constant bit rate. The packets are routed using Ad hoc On-demand distance vector routing protocol and the acknowledgments are authenticated using RSA algorithm.

TABLE I. SIMULATION PARAMETERS



Parameter Name	Parameter Value
Simulation tool	NS-2.28
Simulation area	1216 x 743
Simulation time	70ms
Number of nodes	50
Mobility speed	10ms
Maximum packets in interface queue	100
Propagation model	Two ray ground
Antenna	Omni directional
Traffic model	CBR
Routing protocol	AODV

In order to measure and compare the performance of our proposed scheme, we adopt the following performance metrics:

1) Packet Delivery Ratio: Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources.
2) Delay: Network delay is an important design and performance characteristic. The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another.
3) Routing Overhead: Routing overhead refers to the ratio of routing related transmissions.

VI. PROBLEM IDENTIFICATION

A. SIMULATION ENVIRONMENT

Based on the simulation parameters defined, the mobile ad hoc network is designed as in fig. The existing EAACK algorithm is implemented in this environment and its performance is analyzed.

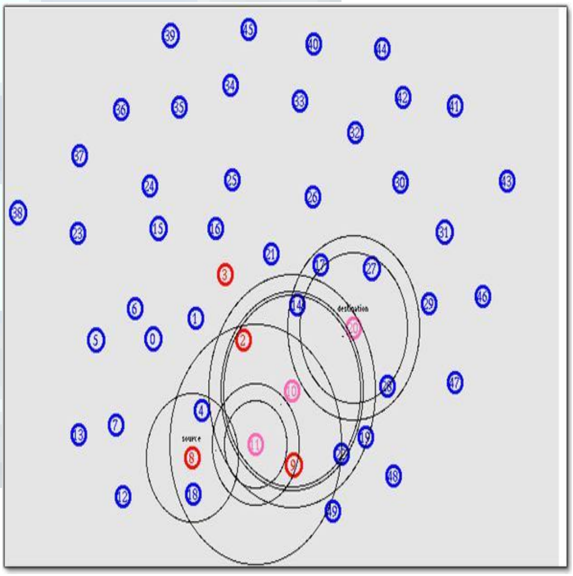


Figure 1: Simulation Environment.

From fig. 1 there are 50 nodes, of which the source node is node 8 and the destination node is node 20. The data is being transferred from source 8 to destination 20 via the route 8-11-10-20. Based on the behavior of algorithm, graphs are generated for the performance metrics routing overhead, delay, packet delivery ratio, packet loss ratio.

B. RESULTS

The graph results obtained after the execution of existing EAACK algorithm for various performance metrics are as follows. Fig. 2, 3 and 4 shows how the performance of EAACK degrades in scenarios of link breakage, source maliciousness and partial packet dropping.

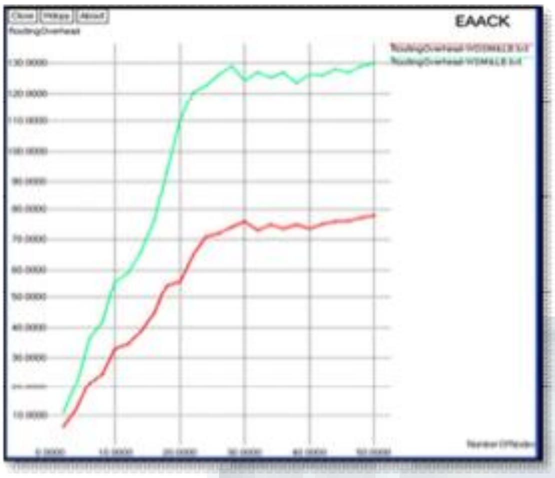
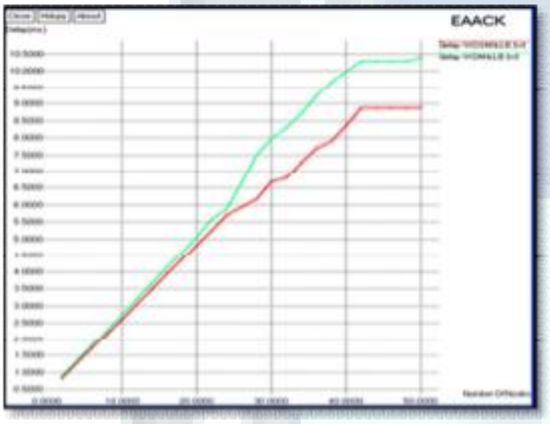


Figure 2: Routing overhead



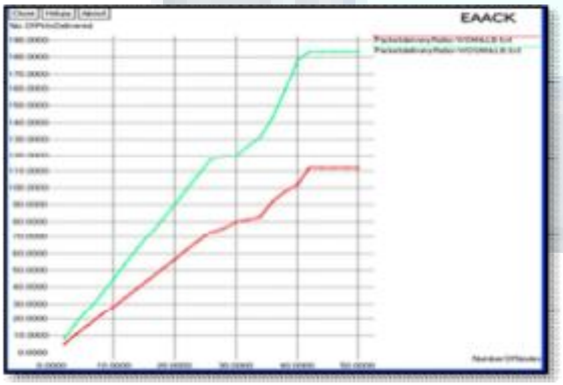


Figure 4: Packet delivery ratio

LEGEND	
🟩	Normal scenarios
🟥	In identified scenarios

The graphs depict that the routing overhead and delay increases while packet delivery ratio reduces in cases of link breakage, source maliciousness and partial packet dropping. These graph results clearly shows the inefficiency and unreliable nature of EAACK algorithm in specific attacks. Further, the network performance degrades as it tries to tackle the network attacks.

C. INFERENCE

From the results obtained, the following inference has been derived.

TABLE II. INFERENCE FROM EXISTING EAACK

PARAMETERS	PERFORMANCE
	Existing EAACK During Link Breakage, Source Maliciousness, and Partial Packet Dropping
Routing Overhead	Increased by 42.3%
Delay	Increased by 7.69%
Packet Delivery Ratio	Decreased by 36.97%

In this project, we aim to improve the security of network against intrusion detection by modifying the existing EAACK algorithm to withstand various attacks from malicious nodes. This will enhance the network reliability.

VII. PROPOSED SCHEME DESCRIPTION

A. RESISTANCE TO ATTACK BY MALICIOUS NODES

Scenario 1:

Under link breakage, the existing EAACK scheme fails. Hence, in our proposed scheme, every node maintains a neighbor list. And this list gets updated periodically, so that when nodes move out of communication range, it is identified. Therefore, if that node moves out of communication range, it will not be able to send an acknowledgment to the source. But, still since the neighbor list is being updated periodically, the source will not classify this node as a malicious node.

On the other hand, the existing EAACK algorithm does not verify the network condition and thereby identifies the node as a malicious node.

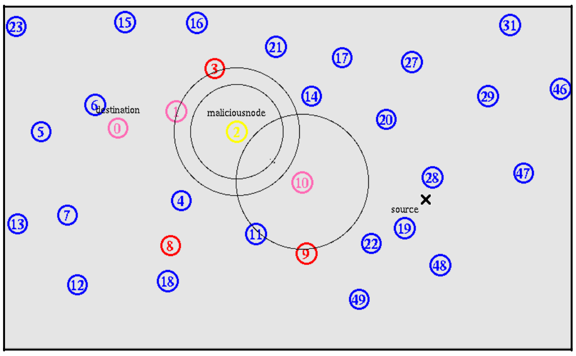
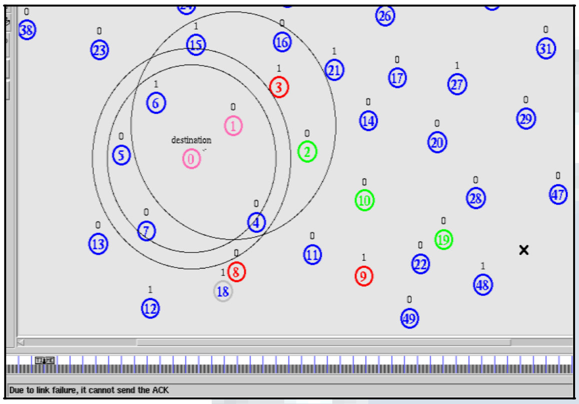


Figure 5: Existing EAACK under link breakage

Fig. 5 shows the implementation of existing EAACK algorithm. Here, the transmission is from source 19 to destination 0. Since, node 2 has gone out of communication range (high mobility), it is not able to send an acknowledgment to node 10. But, the EAACK algorithm is not able to detect it and hence it is unnecessarily marked as a malicious node (marked yellow).

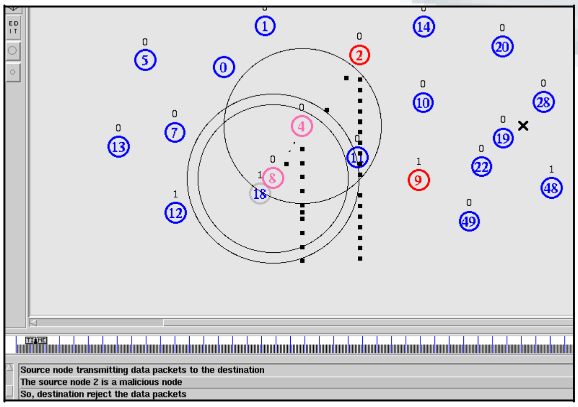


Due to link failure, it cannot send the ACK

Figure 6: Improved EAACK under link breakage

While our improved EAACK has identified that due to link breakage, node 2 has not responded. Hence, it is not a malicious node. Therefore, it has been marked green with the comment "Due to link failure, it cannot send ACK".

Scenario 2:
In existing EAACK algorithm, every decision about the intruders is made by the source. Hence, if source is itself an attacker, EAACK has no provision to identify it. Hence in our proposed scheme, the behavior of every node is recorded and stored as a table. Every node in the network maintains this table about the past history of every other node in the network.



Source node transmitting data packets to the destination
The source node 2 is a malicious node
So, destination reject the data packets

Figure 7: Improved EAACK under source maliciousness

Therefore, if the source node is malicious and tries to send data to the other nodes in the network, the nodes will first check the table to find if the node is a malicious node. If that node has already been marked malicious, the

In order to overcome partial packet dropping, an algorithm called iterative classification algorithm is considered.

Every node sends data as packets to another node. If a node is given packets beyond its queue capacity, that node drops the packet sent. But, certain nodes purposely drop packets for their own benefits. Such, a node is called a partial packet dropper.

Using tcl command, the packet dropping rate of every node is calculated and stored in a file. The average of the entire node's packet dropping rate is taken and is fixed as the threshold value. Any node exceeding this threshold value will be identified and classified as a partial packet dropper.

In addition to this, the time a link exists between every two nodes in the network is calculated and the values are stored as a matrix. Nodes that exceed the threshold limit as well as those nodes that are in link with the malicious attackers (from matrix) for a longer duration are identified. These adversary nodes are assigned a state variable of 1 and the normal nodes are given a state variable 0.

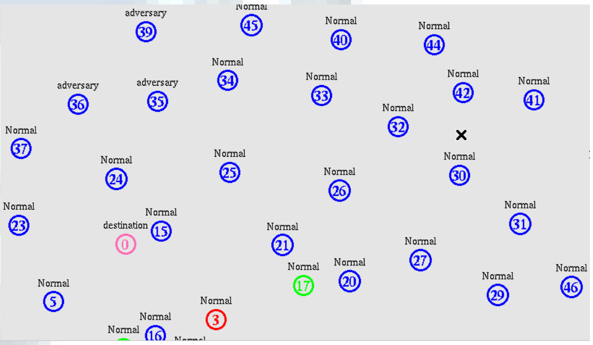


Figure 8: Improved EAACK-partial packet dropping

Thus, from fig. 8 it is clear that improved EAACK has identified the partial packet droppers in network and marked them as adversary.

B. MERITS
Thus, the improved EACK works successfully in

data from that node is dropped as in fig.

Scenario 3:
Iterative classification algorithm
1) Detecting malicious nodes during link breakage, source maliciousness
2) Identifies partial packet droppers
3) Overcomes receiver collision
4) Tackles limited transmission problems
5) Identifies forged acknowledgments and false

misbehavior report.

VIII. PERFORMANCE EVALUATION

A. RESULTS

Thus, based on the individual graphs obtained we have generated a comparison graph for the purpose of evaluating the performance of existing EAACK with our proposed EAACK algorithm as shown in fig. 9, 10 and 11.

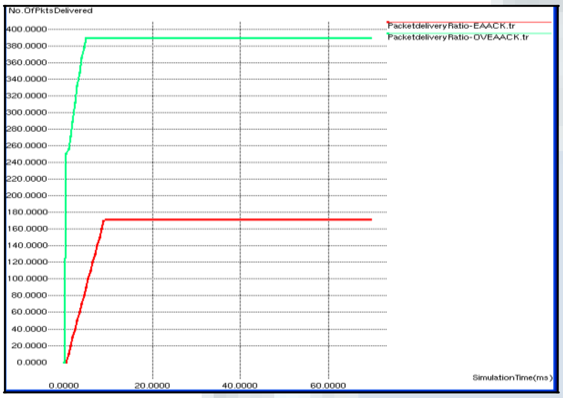


Figure 9: Comparison-packet delivery ratio

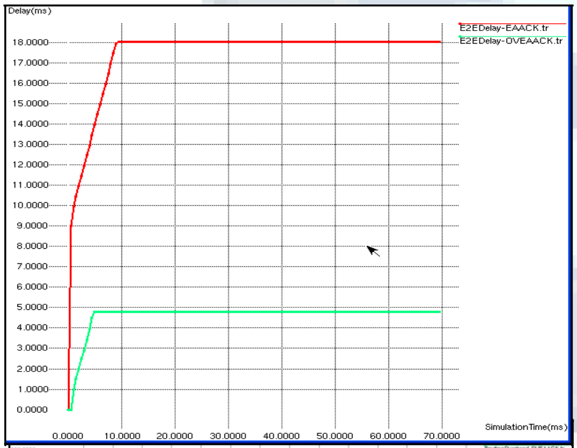


Figure 10: Comparison- delay

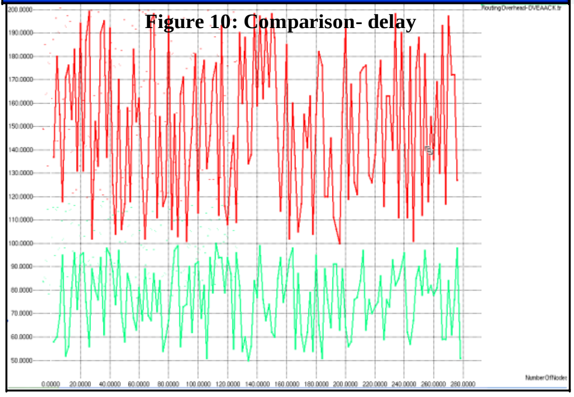


Figure 11: Comparison- routing overhead

our improved EAACK scheme. The following table has been derived from the graph results obtained during the execution of existing and proposed scheme.

TABLE III. INFERENCE FROM IMPROVED EAACK

PARAMETERS	PERFORMANCE
	Proposed improved EAACK In comparison to existing EAACK
Routing Overhead	Reduced by 52.2%
Delay	Reduced by 60.4%
Packet Delivery Ratio	Increased by 56.4%

CONCLUSION AND FUTURE WORK

The above graphs show that the network performance is enhanced using our improved EAACK algorithm (marked green in graph) Intrusion detection has posed a major threat in MANETs for years. In our project we have taken efforts to mitigate various network attack issues like partial packet dropping, forged acknowledgments, false misbehavior reports, receiver collision, and limited transmission. Also, the algorithm handles situations of link breakage and source maliciousness. Apart from detecting malicious nodes in MANETs, the improved EAACK also takes care of network performance as the performance metrics routing overhead and delay are reduced while packet delivery ratio is increased. Further, the power required to run the algorithm is also under control. We hope these results will be of some use in future study in this area helping the growing interest and resulting in the invention of new IDSs.

The Improved EAACK was developed after studying EAACK in various environments. It can be checked in various other scenarios for improvements. Also, hybrid cryptography techniques can be applied to reduce network overhead further. Also, the algorithm can be implemented for a real time scenario and tested instead of software simulation.

REFERENCES

[1] www.wikipedia.org/

[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.

[11] D. Johnson and D. Maltz, “Dynamic Source Routing in ad hoc wireless networks,” in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[12] N. Kang, E. Shakshuki, and T. Sheltami, “Detecting misbehaving nodes in MANETs,” in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[13] N. Kang, E. Shakshuki, and T. Sheltami, “Detecting forged acknowledgements in MANETs,” in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[14] K. Kuladinith, A. S. Timm-Giel, and C. Görg, “Mobile ad-hoc communications in AEC industry,” J. Inf. Technol. Const., vol. 9, pp. 313–323,2004.

[15] J.-S. Lee, “A Petri net design of command filters for semiautonomous mobile sensor networks,” IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

[16] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehaviour in MANETs,” IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[17] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehaviour in mobile ad hoc networks,” in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.

[18] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC, 1996, T-37.

[19] N. Nasser and Y. Chen, “Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network,” in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[20] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, “On intrusion detection and response for mobile ad hoc Computer and Information Science,vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387.

[21] A. Patcha and A. Mishra, “Collaborative security architecture for black hole attack prevention in mobile ad hoc networks,” in Proc. Radio Wireless Conf., 2003, pp. 75–78.

[22] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, “Securerouting and intrusion detection in ad hoc networks,” in Proc. 3rd Int. Conf. Pervasive Comput. Commun., 2005, pp. 191–199.

[23] R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, vol. 21, no. 2,pp. 120–126, Feb. 1983.

[24] J. G. Rocha, L. M. Goncalves, P. F. Rocha, M. P. Silva, and S. Lanceros-Mendez, “Energy harvesting from piezoelectric materials fully integrated in footwear,” IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 813–819,Mar. 2010.

[25] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, “Video transmission enhancement in presence ofmisbehaving nodes inMANETs,”Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.

[26] A. Singh, M. Maheshwari, and N. Kumar, “Security and trust management in MANET,” in Communications

[27] B. Sun, “Intrusion detection in mobile ad hoc networks,” Ph.D. dissertation,Texas A&M Univ., College Station, TX, 2004.

[28] K. Stanoevska-Slabeva and M. Heitmann, “Impact of mobile ad-hoc networks on the mobile value system,” in Proc. 2nd Conf. m-Bus., Vienna,Austria, Jun. 2003.

[29] A. Tabesh and L. G. Frechette, “A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator,” IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.

[30] M. Zapata and N. Asokan, “Securing ad hoc routing protocols,” in Proc. ACM Workshop Wireless Secur., 2002, pp. 1–10.

[31] L. Zhou and Z. Haas, “Securing ad-hoc networks,” IEEE Netw., vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999. Botan, A Friendly C ++ Crypto Library. [Online]. Available: http://botan.randombit.net/

[32] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[33] TIK WSN Research Group, The Sensor Network Museum—Tmote Sky. [Online]. Available: http://www.snm.ethz.ch/Projects/TmoteSky

[34] “EAACK—A Secure Intrusion-Detection System for MANETs”, Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE

[35] Y. Kim, “Remote sensing and control of an irrigation system using a distributed wireless sensor network,” IEEE Trans. Instrum.Meas., vol. 57,no. 7, pp. 1379–1387, Jul. 2008.