Reduction of Overhead Caused by Enhanced Adaptive Acknowledgement With Broadcast Algorithm for Mobile Ad-Hoc Networks

[1]Kavitha.S, [2]Bharathi.E
[1,2]Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore, India

Abstract
The self configuring mechanism causes several issues in MANET, such as energy utilization, secure routing and node authentication. Security challenge is a primary concern in MANET to provide secure communication. Based on this case, it is very important to develop efficient intrusion-detection mechanisms to protect MANET from attacks. In this paper we propose a new algorithm which reduces the computational overhead of Enhanced Adaptive Acknowledgement and provides energy efficient secure routing in MANET. The proposed scheme reduces the bandwidth overhead caused by extra data with EAACK making up the network as congested and increases in packet delivery ratio of the protocol with secure routing.

Keywords
MANET, AODV, EAACK, Broadcast Algorithm, Security, IDS.

I. Introduction

Mobile ad hoc network (MANET) is a network formed by a set of mobile hosts which communicate among themselves by means of the air. The host will establish their own network dynamically without relying on a support infrastructure or a central administration, and the host cooperates to forward the data in a multi-hop fashion. In a network routing, access control and node authentication are of network functionalities that must be done by node cooperation.

The hosts present characteristics in MANET as constraint resources (processing, memory, bandwidth, energy and others), mobility and wireless communication that limit their capacity on performing dense activities, increasing the dynamism of the network topology and the complexity on providing network management, control and security. Due to Unreliability of wireless links between nodes, constantly changing topology and Lack of incorporation of security features the mobile ad-hoc networks are more prone to suffer from the malicious behavior [11]. To detect the intruders or malicious node in the network Intrusion detection system is used. The main purpose of Intrusion detection system is to detect and report the malicious activity of a node in ad hoc networks. Intrusion Detection System (IDS) collects and analyze audit data for the entire network. Critical node in the network is a node whose failure or malicious behavior disconnects or significantly degrades the performance of the entire network [8, 15]. The transfer of information in the network from the source to destination is made secured by Intrusion detection system.

In this paper a new broadcast algorithm is proposed with the EAACK mechanism which reduces the overhead of EAACK mechanism in AODV protocol and increase the packet delivery ratio. The EAACK scheme [9] is an intrusion detection system which passes the 2b packets for secure transaction which cause extra traffic in the network and sometime exceeds than the bandwidth capacity of the network leads to network congestion. To reduce the network congestion in the protocol the broadcast algorithm is proposed. The protocol is implemented in Ns2 [18].

A. Security Goals for Mobile Ad-hoc Networks

The ultimate goal is to secure the mobile ad hoc network from the existing vulnerabilities is to provide a secure routing protocol [12]. The widely used security schemes [16] to protect the mobile ad hoc network from malicious behaviors are

1. Availability
2. Confidentiality
3. Integrity
4. Authentication
5. Non-reputation
6. Access Control

To achieve the goal, the security approach should provide overall protection that spans the entire protocol stack.

II. Intrusion Detection in MANET

A. Design of Intrusion Detection System

Intrusion detection is a method or a tool that identifies, assess and report unauthorized network activity. It is one part of overall protection system that is installed around a system. Based on the network infrastructure Manet can be configured as either flat or multilayer. The optimal IDS architecture of Manet depends on network infrastructure itself. The main architectures in the network [15] are:

- Standalone IDS,
- Distributed and Collaborative IDS,
- Hierarchical IDS, and
- Mobile Agents for IDS

1. Standalone Architecture

This IDS run on each node to determine intrusions independently. The IDSes on the network has no cooperation and no data exchanged among themselves. This type of architecture is more suitable for flat network infrastructure than multilayered network infrastructure.

2. Distributed and Collaborative Architecture

This type of IDS has a rule that every node in the MANET must participate in intrusion detection and respond to IDS agent that runs on them. The IDS agent detects, collects local events, identify the data for possible intrusions and it also initiate a response independently.

3. Hierarchical Architecture

It is an extended version of the distributed and collaborative IDS architecture. The architecture proposes well in multi-layered network infrastructures and the network is divided into clusters. The architecture contains cluster heads, in some case act as control points as like switches and routers.

4. Mobile Agent for IDS Architecture

This type of IDS uses mobile agents to perform specific task on a nodes behalf the owner of the agents. The architecture allows the distribution fashion for intrusion detection tasks. IDS may be classified as host-based and network based, based on the data collection method.

- Host-based IDS operate on the operating system's audit trails, system and application logs.
- Network-based IDS operate on packets that are captured from network traffic.

B. Classification of Intrusion Detection Schemes

Intrusion is any set of actions that attempt to compromise the confidentiality, availability or integrity of a resource [13] and an intrusion detection system (IDS) is a system which is used for the detection of such intrusions. There are three main components of IDS: data collection, detection, and response of the node. In the literature three types of Intrusion Detection Schemes [8] are used

- Anomaly-Based Intrusion Detection
- Misuse-Based Intrusion Detection
- Specification-Based Intrusion detection

1. Anomaly-Based Intrusion Detection

The first technique is anomaly-based intrusion detection and it profiles the symptoms of normal behaviors of the system such as usage frequency of commands, CPU usage etc., It detects intrusions as anomalies that is the difference from the normal behaviors. Various techniques have been applied for anomaly based detection method, e.g. statistical approaches and artificial intelligence techniques. Defining normal behavior is a major challenge which changes over time and intrusion detection systems must be kept up to date.

2. Misuse-Based Intrusion Detection

The misuse based intrusion detection compares the already known attack signatures with the current system activities. This type is generally preferred by commercial IDSs based on its efficiency and has a low false positive rate. The drawback of the approach is that it will not detect new attacks which may occur over time. The system is only strong as its signature database and this needs frequent updating for newer attacks.

3. Specification-Based Intrusion Detection

In this approach the system contains a set of constraints on a program or a protocol that are specified and intrusions are detected as runtime violations of the specifications. It is introduced as an alternative method that combines the strengths of anomaly-based and misuse-based detection techniques, which provides detection of known and unknown attacks with lower false positive rate [14].

III. Related Work

Marti et al. [1] proposed a reputation-based scheme. It contains two modules called watchdog and pathrater that are implemented at each node in the network that detects and mitigate respectively in MANETs. The watchdog enables misbehavior detection at the forwarding level and link level. Watchdog's accusations are the base for the pathrater that rates every path in its cache and subsequently chooses the path that best avoids misbehaving nodes. The disadvantage of watchdog technique is it may fail to detect misbehavior in the presence of collusion attack, limited transmission power, partial dropping and false misbehavior.

Jorge Hortelano et al. [2] focus on watchdog Intrusion Detection scheme and implemented and have deeply analyzed. .Based on the obtained result Bayesian filtering technique is proposed to filter the noise caused by node mobility in the watchdog monitoring process.

Kashyap Balakrishnan et al. [3] propose network-layer acknowledgment-based schemes, termed as TWOACK and S-TWOACK schemes, which can be simply added to any source routing protocol and this scheme performs better than watchdog IDS is evaluated. The TWOACK scheme detects the misbehaving nodes, and then it seeks to prevent the problem by notifying the routing protocol to avoid them in future routes. The scheme is evaluated by stimulation.

Zhang at al. [4] describe a dynamic probabilistic broadcast scheme, is a combination of the probabilistic and counter-based approach. The scheme for route discovery process is implemented with AODV protocol. The rebroadcast probability is dynamically adjusted based on the value of the local packet counter at each mobile node. So, the P value changes when the node moves to a different neighborhood. To suppress the effect using packet counter as density estimates, two constant values d and d1are used to increment or decrement the rebroadcast probability. However, the critical question is how to determine the optimal value of the constants d and d1.

Lu et al. [5] has proposed Scalable Broadcast Algorithm that determines the rebroadcast of a packet based on the fact that the rebroadcast would reach additional nodes.

Chen et al. [6] proposed Directional Forward Routing with AODV protocol (AODV-DFR), takes the directional forwarding that is used in geographic routing into AODV protocol. When a route breaks the protocol can then automatically finds next-hop node for packet forwarding.

Stann et al. [7] have proposed a Robust Broadcast Propagation protocol to provide the near-perfect reliability for flooding in wireless networks, and the protocol has relatively good efficiency. The author presents a new perspective for broadcasting in protocol by reducing the frequency of upper layer which invokes flooding to improve the overall performance of flooding.

IV. Proposed Scheme

A. Enhanced Adaptive Acknowledgement Scheme

EAACK Intrusion detection system is an IDS which is used to detect all the attacks that take place in the node which acts as route for packet transmission from source to destination in AODV protocol [19]. It is activated in Network layer of the protocol stack. Each node contains its own secret private key and public key and each message is digitally signed for authentic purpose. The proposed scheme identifies when the node becomes malicious due to interaction by other nodes in the network. It identifies the selfish node due energy loss that cannot involve in further packet transmission. When a malicious node is identified packet transmission is stopped and new route discover process is handled by the AODV protocol and transmission of packets are preceded.

The EAACK mechanism is initiated after the route is discovered from source to destination. EAACK address all the attack with three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). Attack in AODV protocol is identified by sending a 2-b packet header by EAACK mechanism. A public key and a private key are generated for

each node and they were all distributed in advance. The Digital Signature (DSA) algorithm [17] is for security process of EAACK to make the 2-b packet more secure so that the packet cannot be hacked by the attacker. The 2-b packet is passes from source to destination in a regular time interval with the public key and the reply acknowledgement for the 2-b packets are generated from destination to source in the given timeline in the reverse order which is completely authentic based on asymmetric cryptography. The 2-b packets are well secure and the attackers cannot hack the ACK report. If the destination node sends the ACK report within a time limit then S-ACK is activated. The S-ACK packet is generated for every three node in the route which is used to reduce the overhead of the EAACK scheme verifies the ACK report by sending the S-ACK packet to the destination. If S-ACK packet fails to report about the node then MRA is activated which finally verifies the node and report its status as normal or malicious node. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious which is verified by MRA report and provides the accurate state of the node.

Enhanced Adaptive Acknowledgement (EAACK) Mechanism

```
        S=Source
        D=Destination
1.      ACK Mode
  If D sends the Acknowledgement within the time (Here 3ms)
  {
   Print: Normal mode
  }
  Else if D does not sends the ACK within the time
  {
2.      // S-ACK mode will be activated
   Sends the MRA report; //Misbehavior Report
3.        //MRA mode
   Print: Reported node as a malicious node
     Else
  {
  Sends ACK Packet
  Print: Normal mode
  }
```

Steps-Description

Step 1: A secret private key and public key is generated in advance and each message is digitally signed with DSA algorithm for authentic process.

Step 2: Sends the ACK Packet 2-b to the nodes from source to destination.

Step 3: The Destination D must send the Acknowledgement packet within the time line.

Step 4: If the node D sends the ACK packet in time then the node is in normal mode.

Step 5: If D does not send the ACK packet in the given timeline, then the S-ACK mode will be activated.

Step 6: If S-ACK reports in time then the node is normal.

Step 7: If S-ACK reports a false misbehavior report or if S-ACK does not report to the source S within the time line, MRA mode is activated.

Step 8: MRA scheme sends the 2-b packet, verifies the node with report provided by S-ACK report.

Step 9: If the node provides the same report as S-ACK then the node is reported as malicious node.

Step 10: If the node D does not contain the packet, then the node is reported normal.

As EAACK is acknowledgment-based IDS used in AODV protocol. All three parts of EAACK are acknowledgment-based detection scheme. All the three parts rely on acknowledgment of packets in order to detect misbehavior activity in the network, and is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. And if the attackers are smart enough to forge acknowledgment packets then all the three schemes will be vulnerable which is prevented by authentication in EAACK mechanism. EAACK requires all the acknowledgment packets to be signed before they are sent out and verified until they are accepted. The proposed scheme provides better security in transmission of packets from source to destination which is authentic and identifies the attacks in the nodes which acts as the route from source to destination.

The EAACK mechanism provides secure transaction when compared to Watchdog and TWOACK intrusion detection system but the computational overhead increases and packet delivery ratio decreases. Packets are to be transferred from source to destination and different types of packets are to be transferred. Overhead refers to network routing information sent by application, which uses a portion of the available bandwidth in a network. The extra data that makes up the network as congested cause overhead.

EAACK process the packets such as ACK, S-ACK, MRA (2b packets, etc) are to be sent that transmits the packets more than the node's capacity creates overhead in network. The broadcast algorithm is added to the routing protocol with EAACK mechanism reduces the routing overhead and increases the packet delivery ratio and provides better quality of service [10].

B. Broadcast Algorithm

The broadcast algorithm is used to reduce the overhead caused due to enhanced adaptive acknowledgement scheme in the protocol. The delay in rebroadcast due to traffic or malicious behavior of the node a route discovery process is to determine in the forwarding order from source to destination. The node which has more common neighbors with the previous node has the lower delay. So, this node rebroadcasts a packet to more common neighbors which knows this fact. Therefore, the rebroadcast delay enables the information that the nodes have transmitted the packet spread to more neighbors is a key process of the algorithm.

The algorithm contains a novel scheme for calculating the rebroadcast probability. The process considers the information's like the uncovered neighbors in the set, local node density and metric of connectivity to calculate process of rebroadcast probability. The rebroadcast probability contains two parts:

1. The additional coverage ratio is the ratio of the number of nodes that should be covered by a single broadcast to the total number of neighbors.
2. The connectivity factor reflects the relationship of the network connectivity and also the number of neighbors of a given node.

Broadcast Algorithm Description

Packet: Packet is received from node s.

Rs.id: the unique identifier (id) of RREQs.

Nei(u) : Neighbor set of node u.
UnC(u,x) : Uncovered neighbors set of node u for RREQ whose id is x
T(u,x) : Timer of node u for RREQ packet whose Id is x.
RBD : Rebroadcast Delay
BD : Broadcast Delay
RBP : Rebroadcast Probability

Rebroadcast Delay

Compute uncovered neighbors set UnC (node, Rs.id) for Packet
1. UnC (node, Rs.id) = Nei(node) – [Nei(node) union Nei(s)] – {s}
2. Calculate the Rebroadcast delay RBD
3. BD = 1-|Nei(s)Intersection Nei(node)|/|Nei(s)| ;// Rebroadcast Delay
4. RBD = MaxDelay * BD
5. Set a T(node, Rs.id))

If Neighbor node receives a duplicate Packet from node before T(ni, Rs.id) expires
1. Adjust UnC (node, Rs.id)
2. UnC(node, Rs.id) = UnC(node, Rs.id) – [UnC(node, Rs.id) Intersection Nei(node)]
3. Discard (Packet)

Rebroadcast Probability

If T(node, Rs.id) Expires do
1. Rebroadcast Probability RBP
2. R(node) = |UnC(node, Rs.id)|/|Nei(node)|
3. F(node) = Nc/|Nei(node|
4. RBP = F(node) . R(node)

The algorithm is based on neighbor coverage to reduce the overhead in AODV protocol with EAACK mechanism. The neighbor coverage knowledge includes additional coverage ratio and connectivity factor. The scheme dynamically calculates the rebroadcast delay, which in turn is used to determine the forwarding order and more effectively exploit the neighbor coverage knowledge. Based on less redundant rebroadcast, the proposed algorithm mitigates the network collision and contention to increase the packet delivery ratio and decrease the average end-to-end delay.

V. Stimulation Environment

Stimulated results are obtained by implementing AODV protocol with EAACK IDS and Broadcast algorithm in Ns2. EAACK with broadcast algorithm in AODV protocol is used to increase the quality of service of EAACK and provides secure transaction by detecting all the attacks in the nodes within the network. The malicious node is detected with EAACK IDS system and the node is taken out from the route and normal node is exchanged to continue communication between source and destination. The proposed scheme is evaluated based on the metrics such as Bandwidth overhead and Packet Delivery Ratio. The stimulation parameters of the system are shown in Table 1.

Table 1: Stimulation Parameters

Routing Protocol	AODV
Stimulation Time	80 seconds
Simulation Area	1000*1000m
Number of Nodes	42
Propagation Model	Two Ray ground
Minimum Speed	0.25
Traffic Type	CBR
Maximum Packets	50000
Payload Size	512 bytes

A. Performance Analysis

1. The metrics compared for the performance analysis is overhead and Packet delivery ratio. AODV protocol is implementation with EAACK mechanism and Broadcast algorithm. Overhead is analyzed in the fig. 1.

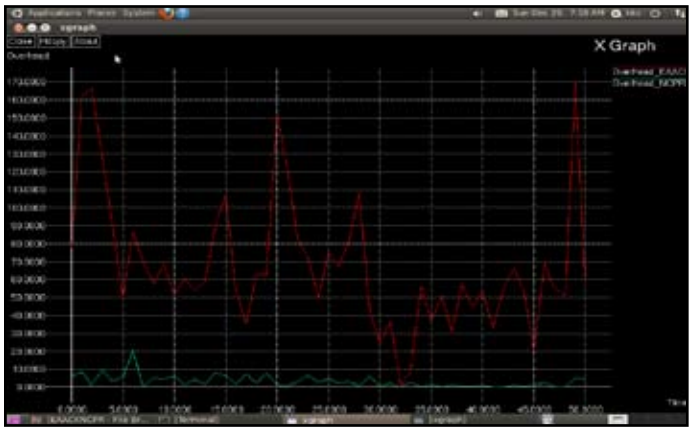

Fig. 1: Comparison of overhead with EAACK and Broadcast Algorithm .

Fig. 1 shows the overhead of EAACK in AODV protocol with Broadcast algorithm. The Read line in the graph indicates increase in overhead, in which the protocol is implemented with EAACK mechanism. The Green line in the graph indicates the reduced overhead,in which Broadcast Algorithm is combined with the protocol with EAACK mechanism. So, Broadcast algorithm provides better performance to reduce the overhead of EAACK mechanism.

2. Packet delivery ratio is an important metric to be compared for better performance of the protocol. Packet delivery ratio with increase in speed without any loss of packet is analysed in the fig. 2.

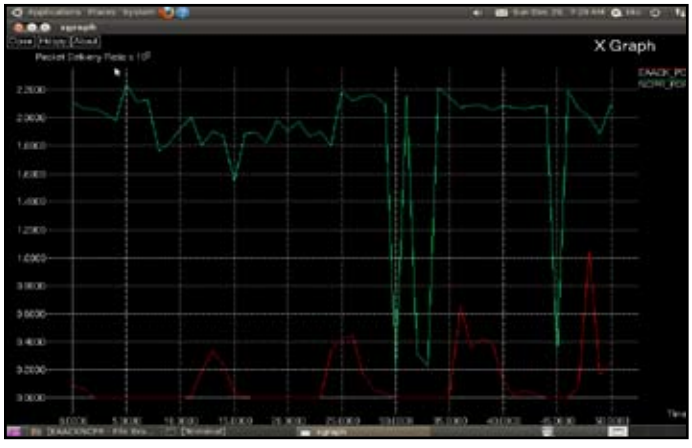

Fig. 2: Packet Delivery Ratio

Figure 2: shows the Packet delivey ratio in AODV protocol with Broadcast algorithm in EAACK mechanism. The Read line in the graph indicates decrease in packet delivery ratio with EAACK mechanism in AODV protocol. The Green line in the graph indicates the increase in packetdelivery ratio with increase based on time and when it reaches 27 sec and 43 sec the packet delivery ratio declines as new route discover process is handled when malicious nodes is identified in the route by EAACK mechanism. Packet delivery ratio increase at the time of 33 sec and 43 sec when packets transmission starts from source to destination.

VI. Conclusion

In this proposed work, the security mechanism for AODV protocol in mobile ad hoc networks is proposed by Enhanced Adaptive Acknowledgement Scheme which is an intrusion detection scheme that detects all the network layer attacks in AODV protocol. The overhead of the protocol caused by EAACK is reduced with the Broadcast algorithm with low overhead and increase in packet delivery ratio. The simulation results also show that the proposed algorithm has good performance in heavy traffic.

References

[1] S. Marti, T.J. Giuli, K. Lai, M.Baker,"Mitigating routing misbehavior in mobile Ad-Hoc networks", 6th MobiCom, Boston, Massachusetts, August.

[2] Jorge Hortelano,"Watchdog Intrusion Detection Systems: Are They Feasible in MANETs", Safewireless.sourceforge.net/papers/watchdog.pdf.

[3] Kashyap Balakrishnan, Jing Deng, Pramod K. Varshney "TWOACK: Preventing Selfishness in Mobile Ad-HocNetworks", IEEE.

[4] Zhang, Q., Agrawal, D.P.: Dynamic Probabilistic Broadcasting in MANETs. Parallel and Distributed Computing. 65, pp. 220–233 (2005) 10.

[5] W. Peng, X. Lu,"On the Reduction of Broadcast Redundancy in Mobile Ad-Hoc Networks", Proc. ACM MobiHoc, pp. 129-130,2000.

[6] J. Chen, Y.Z. Lee, H. Zhou, M. Gerla, Y. Shu,"Robust Ad-Hoc Routing for Lossy Wireless Environment", Proc. IEEE Conf.Military Comm. (MILCOM'06), pp. 1-7, 2006.

[7] F. Stann, J. Heidemann, R. Shroff, M.Z. Murtaza, "RBP: Robust Broadcast Propagation in Wireless Networks", Proc. Int'lConf. Embedded Networked Sensor Systems (SenSys '06), pp. 85-98, 2006.

[8] Vinay P.Virada,"Intrusion Detection System", International Journal of Computational Engineering Research, Vol. 2, Issue 6.

[9] Elhadi M. Shakshuki, Nan Kang, Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transaction on Industrial and Electronics, Vol. 60, No. 3, March 2013.

[10] Xin Ming Zhang, En Bo Wang, Jing Jing Xia, Dan Keun Sung, "A Neighbor Coverage-Based Probabilistic Rebroadcast for Reducing Routing Overhead in Mobile Ad-Hoc Networks", IEEE Transactions on Mobile Computing, Vol. 12, No. 3, March 2013.

[11] MohammadIlyas,"The Handbook of Ad-Hoc Wireless Networks", Handbook.

[12] Frank Stajano, Ross Anderson,"The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, 1999.

[13] Heady R, Luger G, Maccabe A, Servilla M,"The architecture of a network level intrusion detection system", Technical Report, Computer Science Department, University of New Mexico, 1990.

[14] Uppuluri P, Sekar R,"Experiences with Specification-based Intrusion Detection", In Proc of the 4th Int Symp on Recent Adv in Intrusion Detect LNCS 2212: 172-189.

[15] T. Anantvalee, J. Wu.,"A Survey on Intrusion Detection in Mobile Ad-Hoc Networks", Book Series Wireless Network Security, Springer, pp. 170 – 196, 2007.

[16] Hang Zhao,"Security for Ad-hoc Networks", [Online] Available: http://www.cs.columbia .edu/~smb /classes /s09/l26 .pdf

[17] [Online] Available: http://www.en.wikipedia.org/wiki/Digital_Signature_Algorithm.

[18] The Network Simulator ns-2, [Online] Available: http://www.isi.edu/nsnam/ns/.

[19] [Online] Available: http://en.wikipedia.org/wiki/Ad_hoc_On-Demand_Distance_Vector_Routing.

S.Kavitha received her MCA from Bharathiar University on 2011. She is a Research Scholar of Computer Science at Dr. SNS Rajalakshmi College of Arts and Science, presented 2 articles and an international conference. Her area of interest is Network Security, Wireless Network.

E. Bharathi received her Bachelor Degree in computer Science from Bharathiar University in 1997, Master of Computer Application from Bharathiar University in 2000.She received her M.Phil at Periyar University in 2007.She is an Assistant Professor of Computer Applications at Dr.SNS Rajalakshmi College of Arts and Science. Currently, she is pursuing her Ph.D., degree in Computer Science at Bharathiar University. She presented more than 10 papers in various International and National Conferences and published 6 Articles and her Area of Research is Network Security.