International Journal of Advance Research in Science and Engineering
Vol. No. 5, Issue No. 08 , August 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

SECURE ROUTING AND INTRUSION DETECTION ANALYSIS OF BLACK HOLE ATTACK ON MANETS USING NS-2

Sourabh Tilthiya[1], Dr. Sanjay Kumar Sharma[2]

[1] *Department of Electronics and Communication, Research Scholar, UIT-RGPV-Bhopal, M.P, (India)*

[2] *Department of Electronics and Communication, Professor, UIT-RGPV-Bhopal, M.P, (India)*

ABSTRACT

Wireless networks are gaining popularity to its peak today, as the user's wants wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It's an analogy to that of the black hole in the universe in which things disappear. The node presents itself in such a way to the node that it can attack others nodes and networks knowing that it has the shortest path [4]. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed.

Our Intrusion Detection and Response Protocol for MANETs have been demonstrated to perform better than the ones proposed by Stamouli et al in terms of false positives and percentage of packets delivered. Since Stamouli et al do not report true positive i.e. the detection rate, we could not compare our results against that parameter with their method. The implementation of the IDAODV protocol has shown its feasibility to work in real life scenarios; IDAODV performs real-time detection of attacks in MANETs running AODV routing protocol. The prototype has also given some insight into the problems that arise when trying to run real applications on an Ad Hoc network.

Keywords: MANET, Black Hole, Routing protocols, AODV, NS-2.

I. INTRODUCTION

A MANET is known as mobile ad-hoc networks collection of mobile nodes without having any infrastructure or central control. It is characterized by ad-hoc due to dynamic nature of network topology and node specification. Here, node may leave and join the network with wireless communication media as per application requirement. Challenges in such networks is to protect the network from attackers who can attack on network and have

unauthorized access to all information, may theft the private data and use it in unethical manner or may forge someone identity. On-demand routing protocol has a route discovery process initiated by sender. When a traffic resource needs a route, it initiates a RDP (route discovery process) by sending a route request for the destination (typically via a network-on wide flood) and waits for a route reply. There are various kind of routing protocols are proposed and developed to discover route in dynamic topology based network. On-demand routing protocols may be single path or multipath protocols find various routes from source to destination. Here, Source node advertises the route discovery packet to establish route between sender and receiver. It also uses route repairing mechanism to recover damage routes. The major challenge with AODV routing protocols are they don't have any security policy to detect and avoid security attack. Proposed work focus on to avoid security attack and prevent network from attacker's attempt.

1.2Challenges in Wireless Ad Hoc Networks

The two most significant differences between infrastructure-based and Ad Hoc networks are **a)** communications in Ad Hoc networks are truly peer-to-peer and **b)** the individual nodes that do jobs of their own are also now required to route packets as required. These differences lead to some unique and extremely difficult challenges for Ad Hoc networks. Unlike dedicated routers, hosts in MANETs have limited computational resources and more importantly, being battery-operated, very limited power. Building routing decisions in the general-purpose hosts for constantly changing surroundings is big challenge.

1.3 AD-HOC on Demand Routing Protocol (AODV)

To understand the problem of black hole attack on AODV routing protocol first we understand the some common characteristics and it's working of AODV routing protocol in mobile environment. After that we take a look of the black hole attack, attacking mechanism in the AODV routing protocol. Ad-hoc on-demand distance vector (AODV) routing protocol uses an on demand approach for finding routes for communication such a route is established only when it is required by a source node for transmitting a data packet. It allows all mobile nodes, to pass messages through their neighbors to the node which are not in radio frequency range for communication. AODV protocol does this by discovering the routes along which message and information can be send. AODV protocol take precaution for such routes that they do not contain loops and tries to find the shortest route possible. AODV is also able to handle changes in route and can create new routes if there is an error. AODV defines three types of control message for route maintenance: There are three types of control messages in AODV which are discussed below.

1. Route Discovery
2. Route Reply (RREP)
3. Route Maintenance

II. INTRUSION DETECTION IN MANETS

The success of *MANETs*-based applications depends on many factors, trustworthiness being one of the primary challenges to be met. Despite the existence of well-known security mechanisms, additional vulnerabilities and features pertinent to this new networking paradigm might render such traditional solutions inapplicable. The absence of a central authorization facility in an open and distributed communication environment is a major challenge, especially due to the need for cooperative network operation. In particular, in *MANETs*, any node may compromise the routing protocol functionality by disrupting the route discovery process.

2.1 Intrusion Detection

Intrusion is defined as a sequence of related actions performed by a malicious adversary that results in the compromise of a target system. It is assumed that the actions of the intruder violate a given security policy. The existence of a security policy that states which actions are considered malicious and should be prevented is a key requisite for an intrusion detection system to work.

An intrusion detection system must fulfill the following requirements:

Accuracy: An IDS must not identify a legitimate action in a system environment as an anomaly or a misuse (a legitimate action identified as an intrusion is called a *false positive*).

Performance: The performance of the IDS must be sufficient enough to carry out real-time intrusion detection (real-time means an intrusion must be detected before significant damage has occurred). As per the literature, this should be under a minute.

Completeness: An IDS should not fail to detect an intrusion (an undetected intrusion is called a *false negative*). Arguably this requirement is rather difficult to fulfill because it is almost impossible to have a global knowledge about past, present and future attacks. IDS should however, minimize false negatives.

Fault-tolerance: An IDS must itself be resistant to attacks.

Scalability: An IDS must be able to process the worst-case number of events without dropping information. This point is especially relevant for systems that correlate events from difference sources at a small number of dedicated hosts. As networks grow bigger and get faster, such nodes become overwhelmed by increasing number of events.

2.2 Approaches to Intrusion Detection

Intrusion detection techniques have traditionally been classified into two paradigms, namely *anomaly detection*, also known as behavior-based intrusion detectionand *misuse detection*, also called knowledge-based intrusion detection.

In anomaly or behavior-based detection techniques, historical data about a system's activity and specifications of the intended behavior of users and applications are used to build a profile of the "normal" operation of the system. The

detection process then attempts to identify patterns of activity that deviate from the defined profile; anything that does not correspond to a previously learned behavior is considered anomalous and suggests an intrusion attempt.

III. INTRUSION DETECTION AODV (IDAODV)

In this chapter we propose and discuss IDAODV, an Intrusion Detection mechanism for Wireless Mobile Ad Hoc Networks. IDAODV is based on State Transition Analysis Technique, which was initially developed to model host-based and network-based intrusions in a wired network environment.

Of all the routing protocols proposed for MANETs, AODV has been very popular and has become an Internet standard.

3.1 Assumptions

We make the following assumptions. They are realistic and can easily be realized in a MANETs.

- Every link between the participating nodes is bidirectional
- The MAC addresses of the participating nodes remain unchanged.
- Duplicate MAC addresses are not present.
- Network monitor is able to cover all nodes. Monitors passively listen to the routing messages and are discussed subsequently.
- Nodes can listen to transmissions from immediate neighbors.
- All the participating nodes other than the malicious nodes have the intrusion detection component activated.

3.2 Details of IDAODV

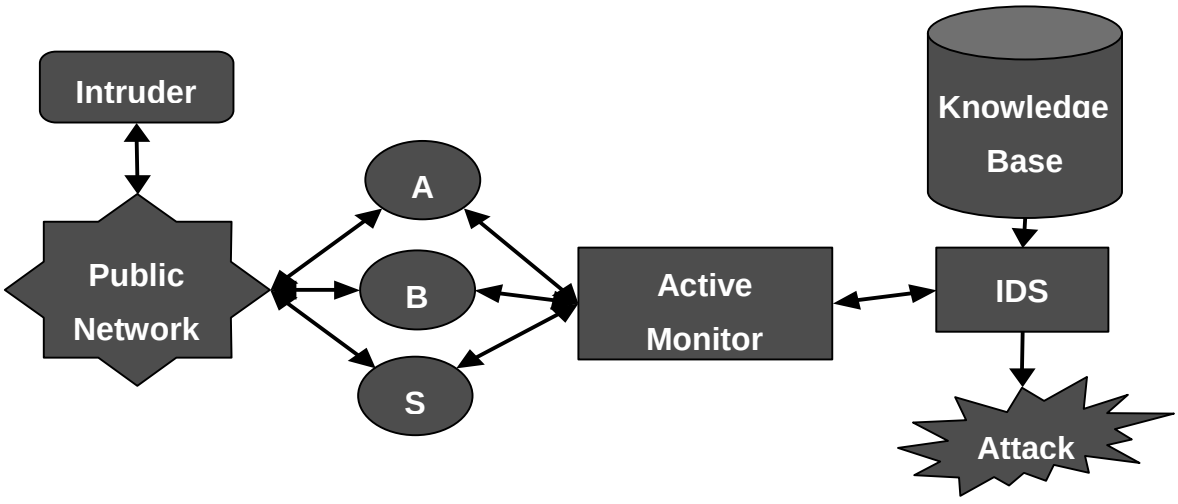

Figure 1: Architecture of IDAODV

3.3 Algorithms

For the intrusion detection to identify the sequence number attack, we analyzed two algorithms.

3.3.1 Notations

The following notations have been used for the description of the algorithms. For a set of paths denoted by **P**, where, path P is an ordered set of nodes, The length of P is defined in terms of number of hops and denoted by |P| For $0 \leq i \leq |P|$, P[i] is the i^{th} node in the path.

3.3.2 Assumptions

The following assumptions have been made for the algorithms.

1. **$\forall$ Pi, Pj$\in$ P, Pi $\not\subset$Pj**
   e.g. if P_1 = {A, B, C} and P_2 = {A, B, C, D}, remove P_1
2. **$\forall$ Pi, Pj$\in$ P, Pi[|Pi| - 1] $\notin$Pj, |Pj|**
   e.g. if P_1 = {A, B, C} and P_2 = {A, B, D, E}, remove C from P_1
3. **$\forall$ Pi $\in$ P, |Pi| > 1**

Algorithm 1: Detection of Routing Packets Dropped

- Check a path from the farthest node to the nearest
- $\forall$ p $\in$ P, check p[|p|]
- If an ACK is received $\forall$ v $\in$ p and v $\neq$ p[|p|], v is *Good*
- Otherwise, check p[|p| - 1]
- If an ACK is not received from p[i+1] but received from p[i], $0 \leq i < |p|$, select p[i]

Algorithm 2: Node Selection

- If p[i] is responsive but p[i+1] is not, there are three possibilities:
  - p[i] is *Bad*
  - p[i+1] is *Lost*
  - The link p[i+1] → p[i] is broken
- Search next shortest path, p_a, to p[i+1] without going through p[i]
- If p[i+1] is responsive, check p[i] over p_a→ p[i+1] → p[i]. If p[i] is responsive, p[i] is *Bad*. Otherwise p[i+1] → p[i] is broken

3.4 Simulation

The experiments were simulated using NS-2. The following section details the simulation environment, metrics and the results.

3.4.1 Simulation Environment

- **Grid Size:** 1000x1000 Meters
- **Packet Traffic:** 10 Constant Bit Rate (CBR) Traffic connections were generated simultaneously. Four nodes were the sources for two streams each, and two nodes were the sources for a single stream each. Destination nodes only receive one CBR stream each.
- **Nodes:** A total of 30 nodes were simulated. Of these, 16 were communicating. Number of bad nodes was varied through the simulation.
- **Mobility:** Random waypoint model was chosen with maximum seed set to 20 meters per second. Pause time was set to 15 seconds.
- **Routing Protocol:** AODV

- **MAC Layer:** 802.11, peer-to-peer MAC Layer model was used.
- **Radio:** We used the 'no fading' radio model with the radio range set to 250 meters.
- **Simulation Time:** 900 Seconds
- **Dropped Packet Timeout:** Timeout period was set to 10 seconds
- **Dropped Packet Threshold:** Set to 10 packets
- **Clear Delay:** Set to 100 seconds, this is an event expiration timer. This is the amount of time for which a node would consider an event before arriving at a conclusion.
- **Modification Threshold:** Set to 5 events
- **Neighbor Hello Period:** Set to 30 Seconds.

IV. RESULTS AND DISCUSSION

4.1 Evaluation of Sequence Number Attack Detection

The four metrics that were used in the evaluation of the Sequence Number Attack Detection and countermeasure mechanism are the delivery ratio, the number of false routing packets sent by the attacker, false positive and detection rate.

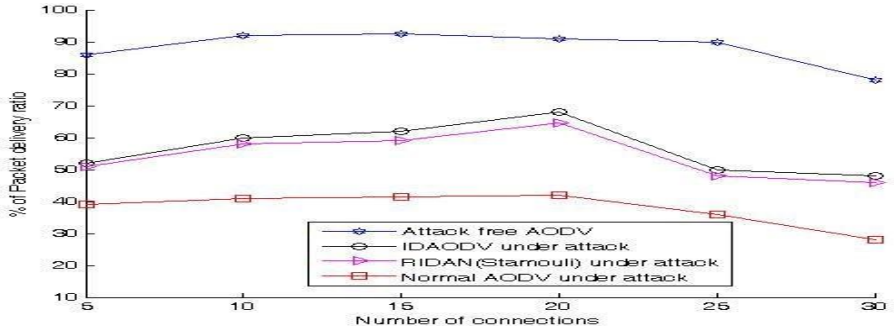

Figure 2: Delivery Ratio Vs Number of Connections

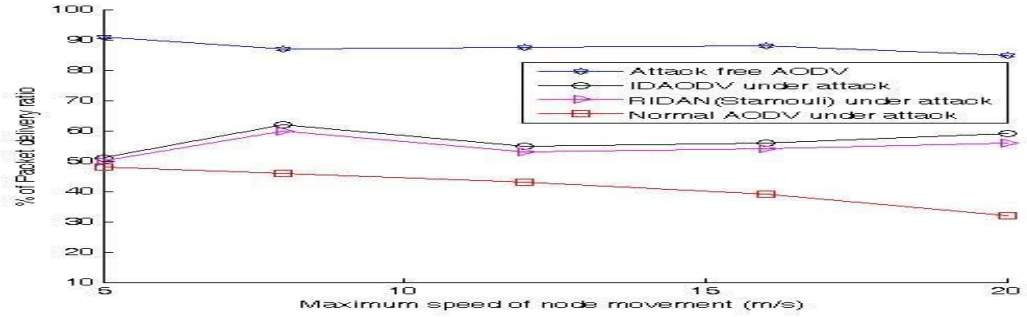

Figure 3: Delivery Ratio Vs Speed of Nodes

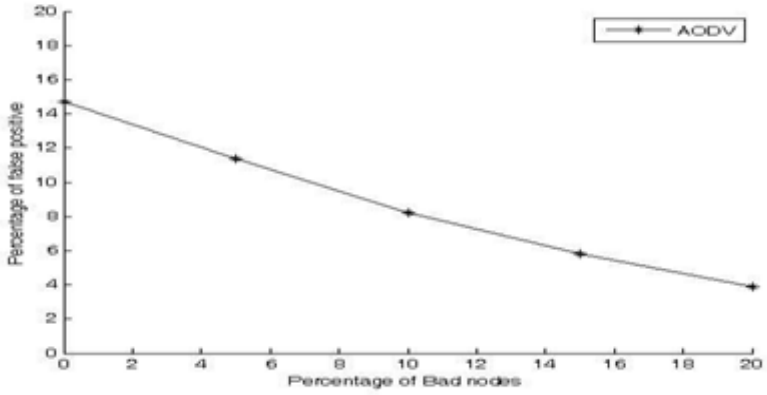

Figure 4: percentage of False Positives Vs percentage of bad nodes

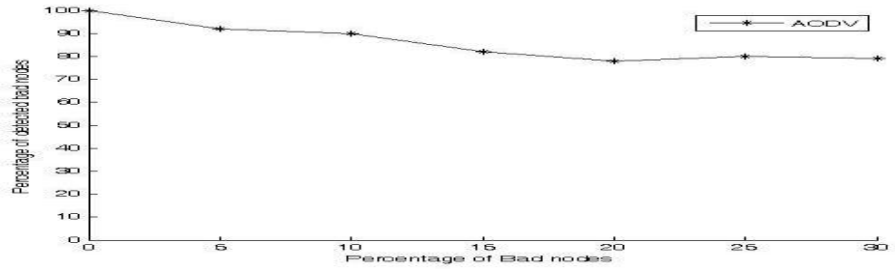

Figure 5: percentage of Detected bad nodes Vs. percentage of bad nodes

4.2 EVALUATION OF THE 'DROP ROUTING PACKETS' ATTACK DETECTION

To evaluate this attack, the metrics chosen were delivery ratio and routing overhead ratio. The following graphs show the performance.

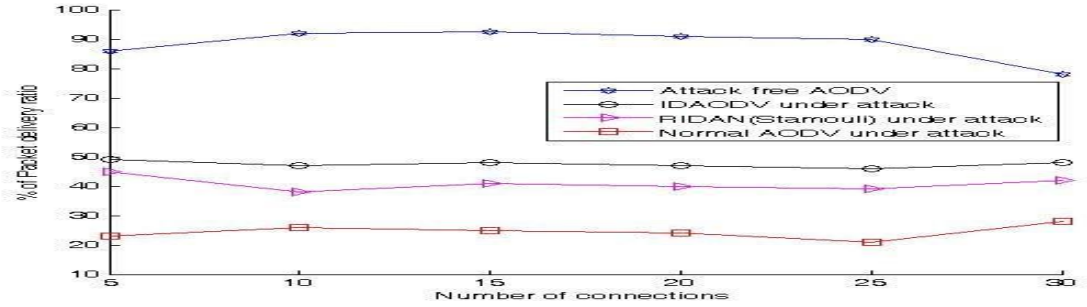

Figure 6: Delivery Ratio Vs. Number of Connections

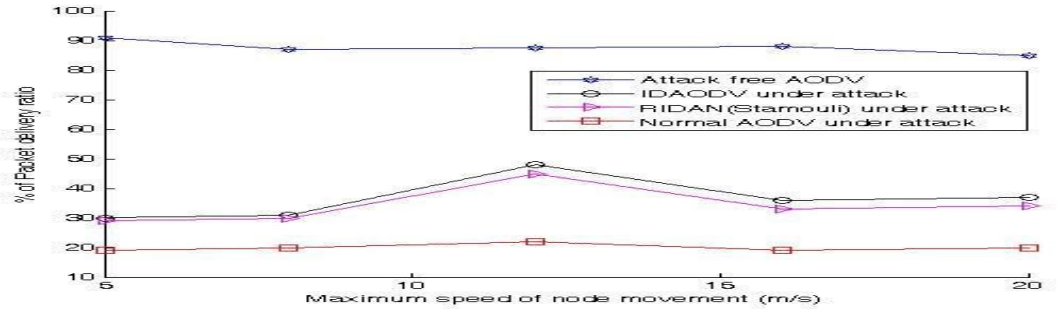

Figure 7: Delivery Ratio Vs. Node Mobility

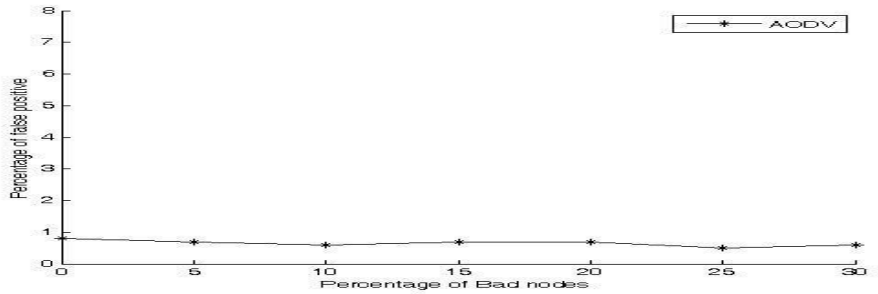

Figure 8: percentage of False Positive Vs percentage of bad nodes

Number of Nodes		20	40	60	80
Static Node case	RIDAN(Stamouli)	52	80	94	98.5
	IDAODV	54	84	96	99.3
Dynamic Node case	RIDAN(Stamouli)	52	80.5	94	99
	IDAODV	57.5	85.1	95	99.8

Table 1: Comparison between RIDAN and IDAODV for % of Detection

V.DISCUSSIONS AND CONCLUSIONS

5.1 Discussions

Stamouli et al [10] have proposed architecture for Real-time Intrusion Detection for Ad Hoc Networks [RIDAN]. The detection process relies on a state-based misuse detection system. In this case, every node needs to run the IDS agent. There is no mention of a distributed architecture to detect attacks that require more than one-hop information. According to the analysis that we performed, the most serious attacks are carried out by 'insiders' who carry out their attacks via an attached terminal, not via the network. Consequently, network-based IDS will fail to detect the most damaging attacks. Moreover, the most pervasive network-based IDSs are signature-based and are only able to detect known attacks. We presented new techniques that advance the field of intrusion detection in several areas. We have designed novel mechanisms to detect and mitigate aberrant behaviors encountered in Mobile Ad Hoc Networks (MANETs). Since MANETs are comprised of resource constrained devices, we designed our intrusion detection mechanisms as protocols that monitor network state rather than system state. We also experimented with reactive protocols for MANETs, extending prior research to work with all mobile Ad Hoc routing protocols, not just AODV. Our experiments and simulations have demonstrated that our protocol is functionally feasible given limited resources.

5.2 Conclusions

An Intrusion Detection System aiming at securing the AODV protocol has been developed using specification-based technique. It is based on a previous work done by Stamouli et al [10]. The IDS performance in detecting misuse of the AODV protocol has been discussed. In all the cases, the attack was detected as a violation to one of the AODV protocol specifications. From the results obtained, it can be concluded that our IDS can effectively detect Sequence Number Attack, Packet Dropping Attack and Resource Depletion Attack with Incremental Deployment. The method has been shown to have low overheads and high detection rate.

REFERENCES

[1] Y.-C. Hu, D. B. Johnson, and A. Perrig, "Sead: Secure efficient distance vector routing for mobile wireless ad-hoc networks," in WMCSA '02: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications. Washington, DC, USA: IEEE Computer Society, 2002, . 3–13.

[2] X. Wang, T. liang Lin, and J. Wong, Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network. Technical Report,Computer Science, Iowa State University, 2005.

[3] J. Grønkvist, A. Hansson, and M. Skøld, Evaluation of a Specification-Based Intrusion Detection System for AODV.di.ionio.gr/medhocnet07/wp content/uploads/papers/90.pdf, 2007.

[4] S. Kurosawa, H. Nakayama, and N. Kato, "Detecting blackholeattackon AODV based mobile ad-hoc networks by dynamic learning method,"International Journal of Network Security, pp. 338–346, 2007.

[5] K. Makki, N. Pissinou, and H. Huang, "Solutions to the black holeproblem in mobile ad-hoc network," 5th World Wireless Congress, pp.508–512, 2004.