DESIGN AND VALIDATION OF SPECIFICATION BASED IDS FOR POWER ENHANCEMENT RELATED VULNERABILITIES IN AODV[1]

Chaitali Biswas Dutta[1], Utpal Biswas2

[1] Research Scholar, Dept of CSE, University of Kalyani, India
Asst. Prof., Dept of CA, GIMT, Guwahati, India
mail.chaitali@yahoo.in

[2]University Of Kalyani, Dept of CSE, University of Kalyani, Nadia, West Bengal, India
utpal01in@yahoo.com

ABSTRACT

Wireless sensor network (WSN) is basically a wireless network, comprised of a large number of sensor nodes which are densely deployed, small in size, lightweight and portable. AODV is a well known, standardized routing protocol used in WSNs. AODV is subject to several attacks like black hole, worm hole, mad in the middle etc. Several Intrusion detection systems (IDS) have been proposed which successfully detect these attacks. Among these IDSs signature based and anomaly based are simple in nature but generate false alarms. To cater to this issue, recently specification based IDS is proposed for WSNs which have low false alarms yet detect most of the attacks. Lots of works have been reported on enhancement of AODV to improve throughput, PDR, NRO, End to End delay, power etc. Power Aware AODV (POW-AODV), enhances WNSs from the perspective of lifetime of nodes (in terms of power). In this paper we show that POW-AODV gets subject to more vulnerability, compared to AODV, in the effort to reduce power. Such attacks reduce life time of nodes instead of increasing them. Following that we propose a specification based IDS for this protocol to detect these vulnerabilities. We also show a using NS-2 simulation that using the IDS POW-AODV leads to increase in lifetime of nodes, even in presence of attacks.

KEYWORDS

Wireless Sensor Network, Ad-Hoc on Demand routing protocol, Fault-Tolerance.

1. INTRODUCTION

Now-a day's wireless technology has become very popular because of the convenience that comes with its use. Wireless sensor network (WSN) [1], [2] is basically a wireless network, is comprised of a large number of sensor nodes which are densely deployed, small in size, lightweight and portable. The WSNs are used in various important fields, like forest fire detection, flood detection, military purposes, tracking and monitoring doctors and patients inside a hospital, home application, commercial application etc. Wireless network is highly dynamic. Topology changes, link breakage, node failure happen quite frequently. That is why routing is an important factor in case of wireless network. If nodes are within the range then routing is not required. Otherwise routing protocol is necessary because routing protocols specify that how routers communicate with each other. Routing protocols in wireless sensor

[1] 1 This journal paper is an extended version of the conference paper "Specification Based IDS for Power Enhancement Related Vulnerabilities in AODV" by Chaitali Biswas Dutta and Utpal Biswas, presented in The Fifth International Conference on Network Security & Applications (CNSA-2012).

DOI : 10.5121/ijnsa.2012.4505

networks are subdivided into proactive routing protocol and reactive routing protocol. Reactive protocols find the route only when there is data to be transmitted. As a result, it generates low control traffic and routing overhead. On the other hand, proactive protocols find paths in advance for all source and destination pairs. Also periodically exchange topology information to maintain them. AODV, DSR are the examples of reactive protocol and OLSR and DSDV are examples of proactive protocol.

Wireless network is not controlled in a centralized manner. It is really tuff to give protection the individual nodes. Inherent properties of ad hoc networks make them vulnerable. Malicious nodes can exploit these vulnerabilities to launch various kinds of attacks. So, Intrusion Detection Systems (IDS) [3] have become an essential component of computer security to detect attacks. IDSs are categorized in two major ways, the first one is based on location of deployment and the second one is based on attack detection methodology. Depending on the location of deployment, again IDSs are classified as Host-based Intrusion Detection System (HIDS) and Network-based Intrusion Detection System (NIDS). Depending on attack detection methodology, IDSs are divided into signature based, anomaly based and specification based. A signature based IDS will monitor data packets of the network and try to match them with the attributes of known malicious threats. Anomaly detection is a process which compares the data packets with some statistics. Signature based and anomaly based IDSs are very popular for a decades. But these two IDSs generate high number of false alarm. Also a few types of attacks are there which neither match with the pattern nor follow the statistics. To avoid this problem specification based IDSs are introduced.

In this paper we give a look on Ad-hoc On-Demand Vector (AODV) [4] routing protocol. Here we will introduce specification based IDS for this protocol. AODV is a very well known standardized reactive routing protocol. AODV's performance is measured in terms of parameters, like throughput, Packet Delivery Ratio (PDR), Normalized Routing Overhead (NRO), End to End delay, power etc. Lots of work has been done on enhancement of AODV to improve the quality of service of these parameters. While these enhancements have improved quality of service in WSNs, they have also lead to new vulnerabilities. Tan et al. have proposed POW-AODV in [32], which is able to provide more throughput than AODV. In this paper we will concentrate on POW-AODV and try to find out the vulnerabilities, also try to develop an event based IDSs for WSNs targeting attacks that arise due to enhancements of routing protocols. We also present the simulation result. Network Simulator (NS-2) has been used for simulation. Through this simulation result we try to prove that after using this detection mechanism the performance of POW-AODV is better than the original.

2. IDS FOR WIRELESS SENSOR NETWORK

Intrusion stands for unauthorized access. The purpose of IDS is to define a boundary between authorized and unauthorized activity. Intrusion Detection Systems (IDSs) detect this type of access. A number of IDSs have been proposed to mitigate various kinds of attacks in WSNs. So, IDS have become an essential component of computer security to detect malicious attacks before they affect the wide network and/or system. There are two major ways for categorization of IDSs – i) based on location of deployment and ii) based on attack detection methodology. Depending on the location of deployment, IDS are classified as Host-based Intrusion Detection System (HIDS) and Network-based Intrusion Detection System (NIDS). A Host-based IDS monitors and analyzes internals of a computing system but a network-based IDS try to detect malicious activities by monitoring network traffic. Depending on attack detection methodology, IDSs are categorized as signature based [5], anomaly based [6] and event/specification based [7]. Signature based IDSs evaluate network traffic for well-known patterns or signatures to detect attacks. Unlike anomaly based IDSs, signature based IDSs have good detection rate only for known attacks. Its drawback is the inability to detect previously unseen attacks. Anomaly

based IDS refer to the problem of identifying patterns in data that do not conform to expected or normal behavior. These non-conforming patterns are often referred to as anomalies, outliers and exceptions. This IDS has two phase–training phase and testing phase. These two detection systems are simple and very well known but both of them generate a high degree of false alarm. But specification based has been proposed as a promising alternative that combine the strengths of misuse and anomaly detection. Specification based IDSs use a set of rules to detect attacks. This IDS has the potential to detect previously unknown attacks. Anomaly based detection is capable of detecting novel attacks, but suffers from a high rate of false alarms. This is the main advantage of specification based system. It generates minimum false alarm in comparison of other two IDS. In this paper, we will apply specification-based techniques to monitor the AODV routing protocol.

3. THE AD-HOC ON-DEMAND DISTANCE VECTOR PROTOCOL

AODV is a well-known reactive and stateless routing protocol used in sensor network. The reactive routing protocols create and maintain routes only on demand. That is, routes between nodes are built when the source node desire. Reactive protocols usually use distance-vector routing algorithms. In our paper we will mainly concentrate on AODV protocol. It uses traditional routing tables and sequence numbers to determine the freshness of routes. An important feature of AODV is that a routing entry not recently used is expired. AODV uses mainly three control packets:

- Routing request message (RREQ) is broadcasted by a node requiring a route to another node,
- Routing reply message (RREP) is unicasted back to the source of RREQ,
- Route error message (RERR) is sent to notify other nodes of the loss of the link

AODV uses periodic HELLO messages to inform the neighbors that the link is still alive. AODV is vulnerable to different kinds of attacks.

When a source node requires a route to a destination it broadcasts a route request (RREQ) packet across the network. After receiving the RREQ a node may unicast a reply message (RREP). This node may be the destination node or may be an intermediate node. If it is a intermediate node then it only rebroadcast the message. If the nodes receive a RREQ which they have already processed, they do not forward it again and discard the RREQ. In AODV sequence number plays an important role. Sequence number Sequence number is increased under two conditions: i) when the source node initiates RREQ and ii) when the destination node replies with RREP. Figure.1 illustrates the flow of the RREQ and RREP messages in a scenario wherein a node A wants to find a route to a node D. (Initially, nodes A, B, C and D do not have routes to each other). Node A broadcasts a RREQ message (a), which reaches to node B. Node B then re-broadcast the request (b). Node C receives the messages and broadcasts the message (c), which arrives at the destination node D. Last, D unicasts back the RREP message to A. We call these RREQ and RREP packets a request-reply flow.

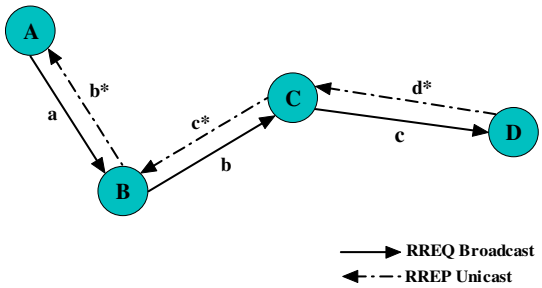


Figure 1: Example of an AODV Scenario

Lots of work has been done on enhancement of AODV to improve quality of service. Performance of AODV have been measured in terms of parameters, like throughput [8], Packet Delivery Ratio (PDR) [9], Normalized Routing Overhead (NRO) [10], End to End delay [11], power [13]etc. In this paper we will consider the parameter power.

4. ENHANCEMENTS OF AODV FOR POWER AWARE ROUTING AND VULNERABILITIES

Tan et al. [13] have proposed Power Aware AODV (POW-AODV), which is able to provide more throughput than AODV and can make better use of the limited battery power available, is an extension or modified version of AODV. POW-AODV approach considers a cost function based on the availability of the battery power. Here, the cost function of the overall route is the sum of the cost functions of the individual nodes along the route. The aim of PAW-AODV is to apply such an algorithm on AODV that can find a route with the least cost.

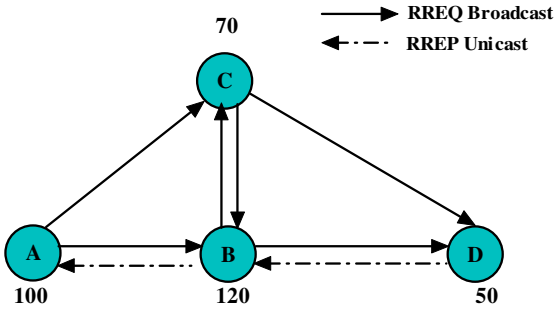


Figure 2: Example to illustrate PAW-AODV

In Figure.2, A, B, C, D are some nodes of the WSN. Values of remaining battery life time corresponding to the nodes are also given in the figure (e.g., 100 Joules for A). RREQ and RREP sequences when A wants to communicate with D are shown in the same figure. In PAW-AODV more than one path from A to D will be found because intermediate nodes do not drop multiple RREQs with same source IP and Request ID.

i) RREQ ABD

ii) RREQ ABCD

The paths are generated are listed below:

i) ABD

ii) ABCD

iii) ACD

iv) ACBD

As discussed before, in POW-AODV cost function depends on the minimum remaining power of a node in a path, which is given in Table 1 for the example of Figure.2.

Table.1: Minimum remaining power of a node in a path for the example of Figure.2

Route	Minimum Remaining Power (Joules)
ABD	100
ABCD	70
ACD	70
ACBD	70

As path ABD has the maximum remaining power it will be considered and RREP will be unicasted through the path DBA.

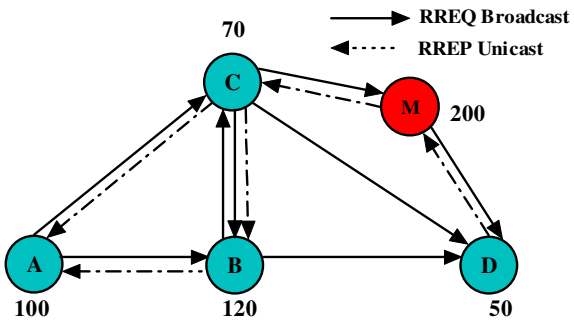


Figure 3: Illustration of an attack against POW-AODV

POW-AODV enhances WSNs from the perspective of lifetime of nodes (in terms of power). However, POW-AODV can be easily exploited by attackers to do the reverse, i.e., use paths having nodes with less remaining battery power, thereby reducing lifetime of some nodes. Figure 3 illustrates such a case. In Figure.3, again we consider the same situation of Figure 2. But here one malicious node M exists between node C and D. In this case, when RREQ reaches D via A,C,M the cost function value should be 70 (due to low remaining power of C), however, M makes it 200 Joules.

This erroneously tells D that path "ACMD" can be taken considering remaining battery life time perspective. It may be easily noted that this path would lead to depletion of power of node C much faster than expected.

In this paper we will propose a scheme which will detect that type of malicious attacks. A number of Sensor Monitors observe the networks and maintain some search table from which monitor can say that this is a malicious attack or not. Then we try to resolve this problem.

5. SPECIFICATION BASED IDS FOR VULNERABILITIES OF POW-AODV

A sensor network is composed of a large number of sensor nodes. Sensor Monitors (SMs) observe and tracing RREQ and RREP messages in a request-reply flow and also try to detect unauthorized access. One SM covered a few number of sensor nodes. Each request-reply flow could have several branches and network monitor maintains a sensor table to trace the branches. When this monitor observed a new request (RREQ) packet, it searches the sensor table and tries to collect the details of the new packet. If SM is failed to match this current packet with the previous packet in sensor table, it contacts with its' neighbor SMs. If one of neighboring monitor give response, SM receives the details of its' previous packet as well as insert a new entry into the sensor table. Otherwise monitor consider it as an attack. Similarly, SM is also efficient to detect anomaly in case of reply (RREP) message. In case of AODV nodes receive a RREQ which they have already processed, they just drop the packet. Since, PAW-AODV wants to find a route with the least cost. So, it allows RREQ message to proceed even if this message has already processed. A SM then employs a finite state machine (FSM) to find out unmatched request or/and reply messages. Before discussing about the function of this state machine we have to enlist some basic assumption. May be these assumptions minimize the area of applications but in this paper we wish to work with these limitation. Basic assumptions are listed below:

- The MAC address of the nodes & the associated IP addresses are fixed & real, a table is maintained by the network monitors which contain the addresses.
- The network monitors pass messages securely & are authenticated to protect against spam.
- Every node must forward or respond messages to its neighbor using some protocol which must be performed within some time threshold.
- Every node must be under the preview of one network monitor at a particular instant of time which can be changed dynamically.
- There may be few nodes not responding the broadcast message, which will not affect the usual functionality.

5.1. Basic Block Diagram of a Sensor Monitor

Sensor network is comprised of a large number of sensors which is monitored by some sensor monitors. Sensor monitors observe route request (RREQ) and route reply (RREP) messages. Figure 4 illustrates the block diagram of sensor monitor.

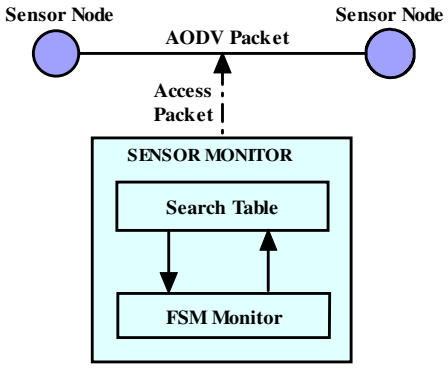


Figure 4: Basic Block Diagram of Sensor Monitor

A sensor monitor maintains the record of the RREQ and RREP messages last received by each monitored node. Sensor monitors are stored the records as in a table format, which is called sensor table. When SM observes a new AODV packet it searches its sensor table and try to find out the previous packet of this packet. If sensor table is cannot provide the data to match the current packet with its previous packet then it will ask its neighboring monitors. If SM receives answer from one of its neighboring SM then no problem but if SM is unable to trace the previous packet then it detects it as an unauthorized access. SM also can mark out the problem like node failure or link failure and mention these as a RRER. Another part of SM is FSM Monitor. Search table decides the state with the help of this FSM monitor.

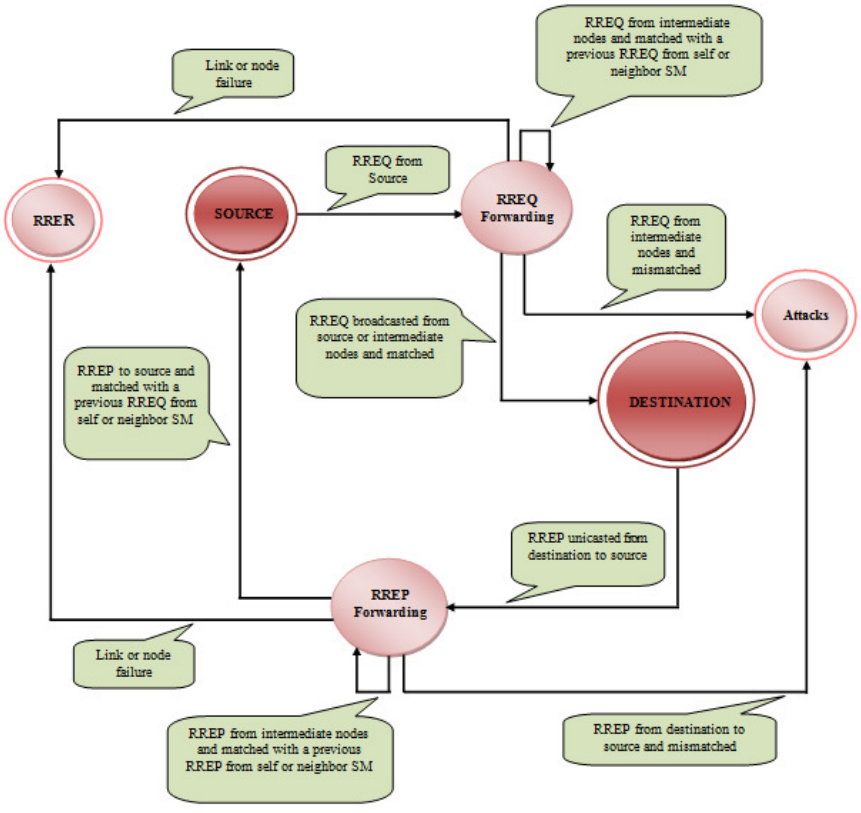


Figure 5: FSM to detect unmatched RREQ and RREP messages

5.2. Working Steps of Finite State Machine

Each sensor monitor uses a finite state machine (FSM) for detecting unauthorized RREQ and RREP messages. Figure 5 describes that type of state machine.

1. RREQ message is broadcasted from the source and go to RREQ Forwarding state.
2. When a packet move from one node to another node than sensor monitor sniff this packet and match with the sensor table.
3. If sensor monitor is able to find out that this packet is already registered then it allows the packet to move further.
4. If packet is not matched then the sensor monitor asks its neighbor monitors. Neighbor monitors search it in their sensor table. If the monitor get the details of the packet then the monitor update its sensor table and allows the packet to go ahead. But if the detail of the packet is not found then monitor declared this is an incorrect forwarding. Then it goes to Attacks state.
5. If it is matched with the previous record then go to DESTINATION.
6. Reply message is unicasted from destination and go to RREP Forwarding state.
7. Step 2, 3, 4 are also same for RREP packet.
8. If any link or node is nor responding at the time of RREQ forwarding and RREP forwarding.

5.3. An Example to Illustrate the Scheme

The concept is explained below using an example. In Figure 6, three sensor monitors, S1, S2 and S3, work cooperatively and trace the request flow. Node A sends a RREQ message a, which is observed and recorded by S1.

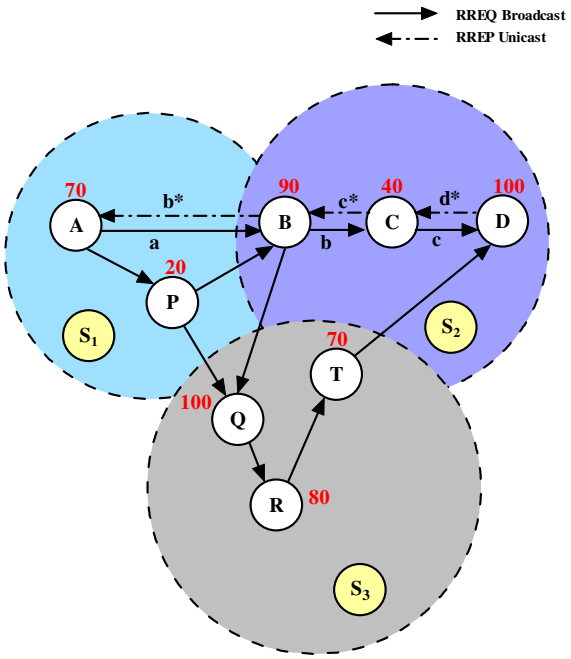


Figure 6: Example of Network Scenario with Network Monitor

Node B accepts this message a. But monitor S2 is unaware about this message. Then first S2 searches its' search table if it is unavailable there them S2 try to verify the information from its neighbor SMs. Then S1 ensure about the existence of message a. Here each RREQ message contains the following field: {Source Address, Request ID, Source Sequence Number, Destination Address, Destination Sequence Number, Hop Count, Minimum Remaining Power}. Let message 'a' has the content {A, r1, 100, D, 61, 0, 70}. There exist a number of routes between node A to node D in Figure 5. Search table contains the record of remaining power of each node as well as the minimum remaining power of each route. In Figure 5, node A's remaining power is greater than B's remaining power, so B also display A's remaining power (which is 70). But C's remaining battery power is minimum than the power declared by node B. So now C's remaining power will contain by the RREQ message. D's remaining battery power is higher than the power declared by the node C. So node C has minimum remaining power and this is the minimum remaining power of the route ABCD. Now we find out the minimum remaining battery power of the routes between nodes A to node D.

Table 2: Minimum remaining power of a node in a path for the example of figure.6

Route	Minimum Remaining Power
ABCD	40
ABQRSD	70
APBCD	20
APBQRSD	20
APQRSD	20

According to this above table 70 is the maximum remaining power among the routes between node A and node D. So routing protocol chooses this route ABQRSD, though its hop count is high. But this can be exploited by malicious node. We consider this type of case in Figure 7.

In Figure 7, again we consider the same situation of Figure 6. But here one malicious node M exists between node T and D. M displayed its remaining battery power very high which is false. But network choose these routes which are through this malicious node. May be hop count will be high of these routes. May be original remaining power is very low of these routes. But network have to recognize this as a malicious attack.

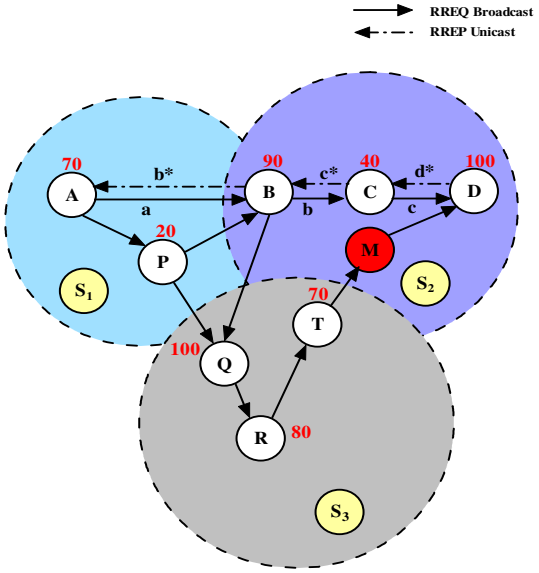


Figure 7: Example of Network Scenario with Malicious Node

A number of sensor monitor like S1, S2, S3 etc. observe the network and maintain the data of the network. For example we consider the route APQRTMD. Sensor monitor S1, S2 and S3 monitor this particular route. Sensor tables also keep the track. S2 observe that the RREQ message coming from A through T contains 20 as minimum remaining battery power. But malicious node M suppressed this value and sends a high value like 200 or something. But sensor monitor can trace this change. Sometimes when a sensor monitor observes that a data packet contain 20 as a minimum remaining power of the route but when this packet go through a particular node it will increase, then monitor detect it as a attack.

6. PERFORMANCE EVALUATION AND DISCUSSION

For the performance evaluation of the developed system, version 2.34 of NS-2 has been used in this paper. Ns-2 is a discrete event simulator targeted at networking research. During the simulation, performance of POW-AODV is compared with that of AODV under different scenarios. Mainly we show here three cases normal case, during attacks and during attack with our attack detection mechanism.

Table 3: Simulation Parameter

Sr. No.	Parameter	Value
1	Simulator	NS-2 (Version 2.34)
2	Channel Type	Channel/ Wireless Channel
3	Traffic Model	Constant Bit Rate (CBR)
4	Source type	UDP, TCP
5	Area (m* m)	2000 * 2000 (initially)
6	Number of Sensor Node	100
7	Simulation Time	5000 s
8	Routing Protocol	AODV, POW-AODV

During the simulation we initially take 2000m*2000m area and 100 nodes are randomly deployed in this area. After that area is gradually increased to 600m*600m, 900m*900m and so on but the number of nodes is fixed in those areas. The initial battery power of each node is set to 20 Joules. Here the rate of packet generation is set to 1 packet/s.

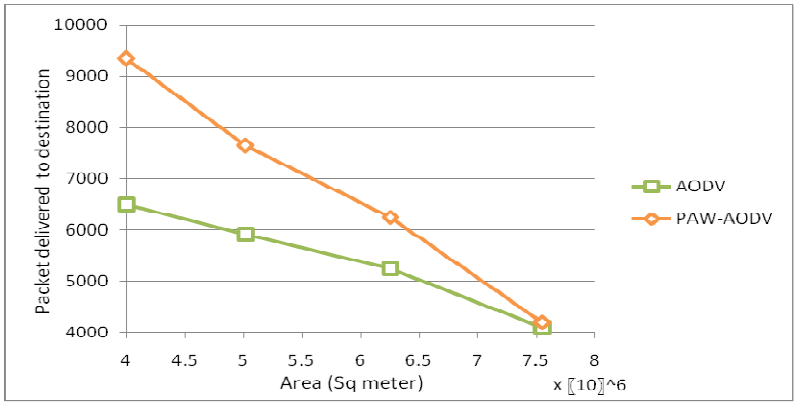


Figure 8. Packet delivery to destination for AODV and PAW-AODV under no attack

Simulation result is shown below by three graphs. The graph, shown by figure 8, describes the rate of data packets deliver successfully at normal time, i.e., no unauthorized access is occurred. POW-AODV has the capability to reduce the power consumption almost 55% in comparison of traditional AODV. As a result around 43%

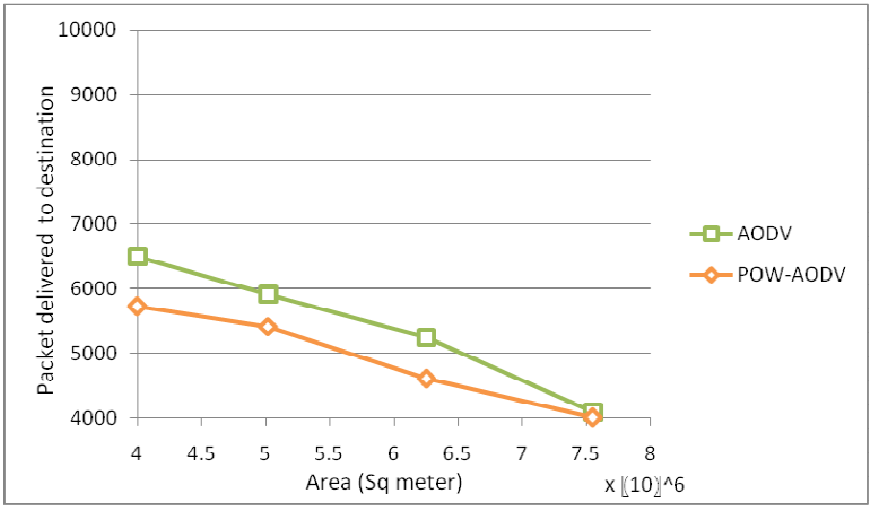


Figure 9. Packet delivery to destination for AODV and PAW-AODV under attack

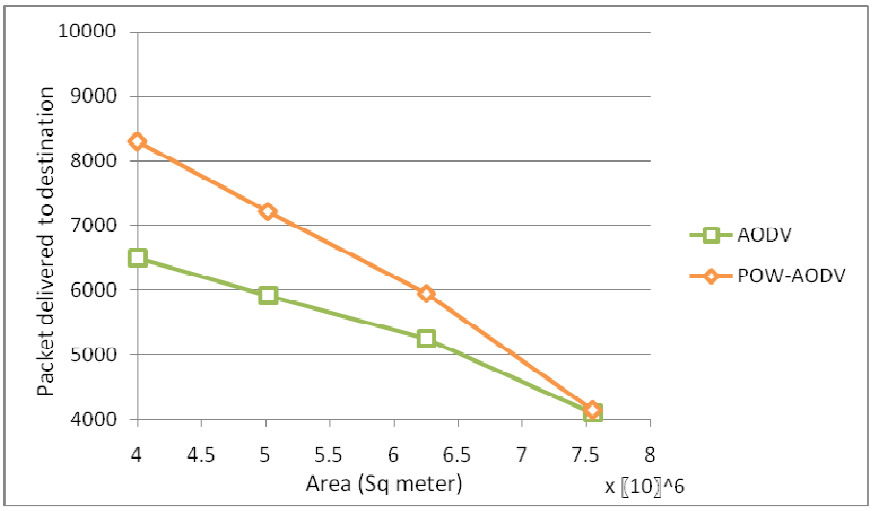


Figure 10. Packet delivery to destination for AODV and PAW-AODV under attack and IDS running

more data packets are successfully delivered to the destination using POW-AODV, when we have considered the size of the area 4*106sq. meter. So we can say that performance of POW-AODV is more better than that of traditional AODV when there is no unauthorized access.

But if attacks will happen then the performance graph of POW-AODV is going down in comparison of traditional AODV. Because POW-AODV is unable to detect any types of attack. This scenario is described by Figure 9.

If power aware AODV is used with our proposed detection mechanism system then it will perform much more better than the original at the time of unauthorized access. The comparison graph of Figure 10 has shown this.

7. CONCLUSION AND FUTURE WORK

In this paper we concentrated on Power Aware AODV (POW-AODV), which is an enhancement of AODV routing protocol to improve the quality of service for wireless sensor network. In normal case it gives far better result than that of traditional AODV. But POW-AODV is not enough concern about unauthorized access. As a result performance of POW-AODV is poor than that of traditional AODV if any malicious attacks will happen. In our paper we state that POW-AODV can hamper by what type of attack. Also try to introduce a detection mechanism system for this protocol. This mechanism system will able to find out the unauthorized access. We have further given a solution after detection of attack. Finally we have verified this scheme using network simulator (NS-2) and have shown that POW-AODV with this detection mechanism perform well than the original at the time of unauthorized access.

In our paper we state the possible vulnerabilities but a number of vulnerabilities can happen. In future we will study the different types of vulnerabilities and try to improve the detection mechanism system for these type of attacks

REFERENCES

[1]. J. Stankovic, “Wireless Sensor Networks”, Handbook of Real-Time and Embedded Systems, CRC, 2007.

[2]. F. L. Lewis, “Wireless sensor networks,” in Smart Environments: Technologies, Protocols, and Applications,D. J. Cook and S. K. Das, Eds. New York: Wiley, 2004.

[3]. Patwardhan, J. Parker, A. Joshi, A. Karygiannis and M. Iorga. “Secure Routing and Intrusion Detection in Ad Hoc Networks”, Third IEEE International Conference on Pervasive

[4]. Computing and Communications 2005.4 On-demand distance vector (AODV) routing, RFC 3561, 2003.

[5]. M. Roesch. Snort - lightweight intrusion detection for networks. In LISA ’99: Proceedings of the 13th USENIX System Administration Conference, pages 229–238. USENIX Association, 1999.

[6]. V. Chandol, A. Banerjee, and V. Kumar. Anomaly detection: A survey. ACM Computing Survey, 41(3):1–58, 2009.

[7]. Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, Jeff Rowe, Karl Levitt, “A specification-based intrusion detection system for AODV,” Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, 2003, page 125—134.

[8]. Alshanyour, Ahed M. and Baroudi, Uthman, “Bypass AODV: improving performance of ad hoc on-demand distance vector (AODV) routing protocol in wireless ad hoc networks”, Proceedings of the 1st international conference on Ambient media and systems, pages 17:1--17:8, 2008.

[9]. Liu, Jian and Li, Fang-min, “An Improvement of AODV Protocol Based on Reliable Delivery in Mobile Ad Hoc Networks”, Proceedings of the 2009 Fifth International Conference on Information Assurance and Security - Volume 01, pages 507—510, 2009

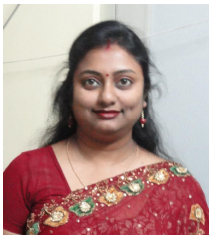
[10]. Chen, Dongru and Wang, Xia, "AODV with lower routing overhead", Proceedings of the 5th International Conference on Wireless communications, networking and mobile computing, pages 2649—2652, 2009.4. Michalewicz, Z.: Genetic Algorithms + Data Structures = Evolution Programs. 3rd edn. Springer-Verlag, Berlin Heidelberg New York (1996)

[11]. Sethi, S. and Udgata, S. K., "SRMAODV: a scalable reliable MAODV for MANET", Proceedings of the International Conference and Workshop on Emerging Trends in Technology, pages 368—373, 2010.

[12]. V. Bharathi, T. Poongkuzhali, "A Performance Enhancement of an Optimized Power Reactive Routing based on AODV Protocol for Mobile AD-HOC Network", International Journal of Technology and Engineering System, page 39-45, Vol2. No 1, 2011.

[13]. Chee-Wah Tan, Sanjay Kumar Bose "Modifying AODV for Efficient Power-Aware Routing in MANETs", IEEE TENCON, 2005, pages 1-6.

Authors



Chaitali Biswas Dutta received the B.Sc. Degree in mathematics from University of Burdwan, India in 2003, the Master of Computer Application degree and MTech degree in Information Technology, both from West Bengal University of Technology, India, in 2006 and 2009 respectively. Currently she is a research scholar in the Department of Computer Science and Engineering, University of Kalyani, India. She is also an assistant professor, department of Computer Application, GIMT, Guwahati, India. Her research interest includes sensor network, wireless network security, VLSI, and so forth. She has published a few papers in international journals and conferences.

Utpal Biswas received his B.E, M.E and PhD degrees in Computer Science and Engineering from Jadavpur University, India in 1993, 2001 and 2008 respectively. He served as a faculty member in NIT, Durgapur, India in the department of Computer Science and Engineering from 1994 to 2001. Currently, he is working as an associate professor in the department of Computer Science and Engineering, University of Kalyani, West Bengal, India. He is a co-author of about 35 research articles in different journals, book chapters and conferences. His research interests include optical communication, ad-hoc and mobile communication, semantic web services, E- governance etc