International Journal of Electrical and Electronic Engineering & Telecommunications

ISSN 2319 – 2518 www.ijeetc.com
Special Issue, Vol. 1, No. 1, March 2015
National Level Technical Conference P&E- BiDD-2015
© 2015 IJEETC. All Rights Reserved

Research Paper

DETECTION OF COLLABORATIVE ATTACKS IN MANETS USING ENHANCED CBDS TECHNIQUE

M Beneto Nixon[1]*, A Swarnalatha[2] and R Avudaiammal[2]

*Corresponding Author: M Beneto Nixon, ✉ nixonbeneto@gmail.com

Mobile ad hoc networks (MANETs) are mainly used for communication between nodes in a network. A major problem to be addressed is the presence of malicious nodes in the network. These malicious nodes may discard the data packets completely or partially. These attacks are called as blackhole and grayhole attacks. These attacks lead to serious security concerns, such nodes may disrupt the routing process. As MANETs are used in different fields like military, medical, etc., preventing or detecting malicious nodes launching grayhole or collaborative blackhole attacks is a challenge. To resolve this issue Dynamic Source Routing (DSR)-based routing mechanism, which is referred to as the Enhanced Cooperative Bait Detection Scheme (ECBDS), that integrates the advantages of both proactive and reactive defense methods. In ECBDS method the destination node involves in the malicious node detection process, thereby avoiding loss of data packets. Simulation results, show that in the presence of malicious-node attacks, the ECBDS outperforms the existing DSR protocols in terms of packet delivery ratio and routing overhead.

Keywords: MANETs, CBDS, DSR, Blackhole and grayhole attacks, Packet delivery ratio, Routing overhead

INTRODUCTION

A Mobile Adhoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others needs the aid of intermediate nodes to route their packets. Each of the node has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices

[1] Department of Applied Electronics, St. Joseph's College of Engineer, 600119, India.

[2] Department of ECE, St. Joseph's College of Engineer, 600119, India.

frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

MANETs are a kind of wireless ad hoc network that usually has a routable networking environment on top of a link layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network in contrast to a mesh network which has a central controller.

RELATED WORKS

In this paper [1], Securing Ad Hoc Networks, Lidong Zhou and Zygmunt Haas have studied the threats an ad hoc network faces and the security goals to be achieved. They identified the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication. In particular, taking advantage of the inherent redundancy in adhoc networks, multiple routes between nodes to defend routing against denial-of-service attacks. They also use replication and new cryptographic schemes, such as threshold cryptography, to build a highly secure and available key management service. In this paper [2], SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, Yih-Chun Hu, David Johnson and Adrian Perrig have designed and evaluated the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol (DSDV). In this paper [3], On Intrusion Detection and Response for Mobile Ad Hoc Networks, James Parker, Jeffrey Undercoffer, John Pinkston, and Anupam Joshi have presented a network Intrusion Detection (ID) mechanism that rely upon packet snooping to detect aberrant behaviour in mobile ad hoc networks. They are applicable to several mobile ad hoc routing protocol, offer two response mechanisms, passive to singularly determine if a node is intrusive and act to protect itself from attacks, or active to collaboratively determine if a node is intrusive and act to protect all of the nodes of an adhoc cluster. In this paper [4], An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs, Kejun Liu, Jing Deng, Pramod Varshney and Kashyap Balakrishnan proposed the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehaviour and to mitigate their diverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In this paper [5], Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks, Nidal Nasser and Yunfeng Chen overcomes the weakness of Watchdog and introduce our intrusion detection system called ExWatchdog. The main feature of the proposed system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. In this paper [6], Anonymous Communications in Mobile Ad

Hoc Networks, Yanchao Zhang, Wei Liu and Wenjing Lou proposes a novel anonymous on-demand routing protocol, termed MASK, to enable anonymous communications thereby thwarting possible traffic analysis attacks. Based on a new cryptographic concept called pairing, he first propose an anonymous neighbourhood authentication protocol which allows neighbouring nodes to authenticate each other without revealing their identities.

PROPOSED MODEL

The need for the work is to overcome the challenges faced by MANETs. The performance of the MANETs completely degrades due to various attacks caused during the transmission of packets. These attacks must be avoided in order to get high throughput and performance during data transmission. Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET.

In this method the hacker node is found by comparing the RREP message sent by all the nodes to the source node. If a node's other nodes reply, then it is determined as the hacker node.

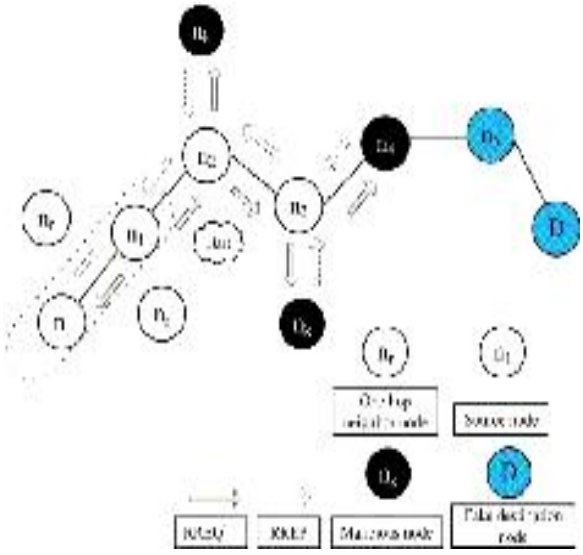
Cooperative Bait Detection Scheme (CBDS)

In our technique a detection scheme called the Cooperative Bait Detection Scheme (CBDS), which aims at detecting and preventing malicious nodes launching grayhole/ collaborative blackhole attacks in MANETs. In our approach, the source node stochastically selects an adjacent node with which to cooperate, in the sense that the address of this node is used as bait destination address to bait malicious nodes to send a reply RREP message. Malicious nodes are thereby detected and prevented from participating in the routing operation, using a reverse tracing technique.

In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again. Our CBDS scheme merges the advantage of proactive detection in the initial step and the superiority of reactive response at the subsequent steps in order to reduce the resource wastage.

CBDS is DSR-based. As such, it can identify all the addresses of nodes in the selected routing path from a source to destination after the source has received the RREP message. However, the source node may not be necessarily able to identify which of the intermediate nodes has the routing information to the destination or which has the route reply RREP message or the malicious node route reply RREP message. This scenario may result in having the source node sending its packets through the fake shortest path chosen by the malicious node, which may then lead to a blackhole attack. To resolve this issue, the function of HELLO message is added to the CBDS to help each node hop.

Figure 1: Detection of Malicious Nodes Using BAIT Technique



This function assists in sending the bait address to entice the malicious nodes and to utilize the reverse tracing program of the CBDS to detect the exact addresses of RREP malicious message nodes. The baiting is RREQ not packets similar are to the original RREQ packets, except that their destination address is the bait address.

PERFORMANCE METRICS

The performance metrics is used to evaluate our results. Here we choose two metrics, they are PDF and RO.

Packet Delivery Fraction

This is defined as the ratio of the number of packets received at the destination and the number of packets sent by the source.

Here, $pktd_i$ is the number of packets received by the destination node in the i^{th} application, and pktsi is the number of packets sent by the source node in the i^{th} application.

Routing Overhead

This metric represents the ratio of the amount of routing related control packet transmissions to the amount of data transmissions.

Here, cpk_i is the number of control packets transmitted in the i^{th} application traffic, and pkt_i is the number of data packets transmitted in the i^{th} application traffic.

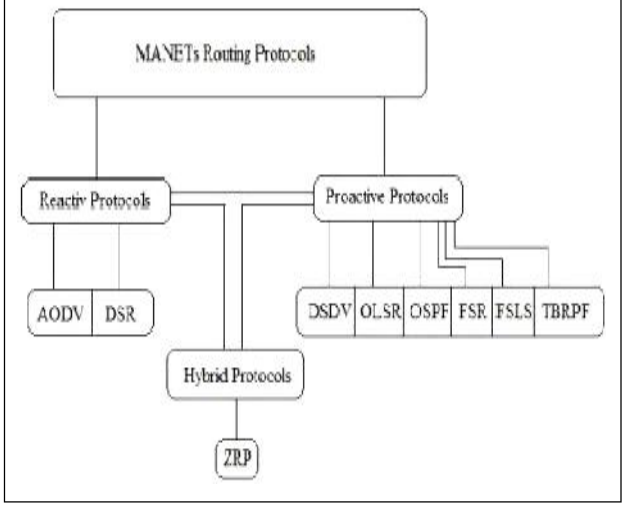
CLASSIFICATION OF ROUTING PROTOCOLS

Routing protocols in MANETs are classified into three different categories according to their functionality. They are,

1. Reactive protocols
2. Proactive protocols
3. Hybrid protocols

The hierarchy of these protocols is shown below,

Figure 2: Routing Protocol



Proactive Protocols

Proactive routing protocols work as the other way around as compared to reactive routing protocols. These protocols constantly maintain

the updated topology of the network. Every node in the network knows about the other node in advance, in other words the whole network is known to all the nodes making that network. All the routing information is usually kept in tables. Whenever there is a change in the network topology, these tables are updated according to the change. The nodes exchange topology information with each other; they can have route information any time when they needed.

Hybrid Protocols

Hybrid protocols exploit the strengths of both reactive and proactive protocols, and combine them together to get better results. The network is divided into zones, and use different protocols in two different zones, i.e., one protocol is used within zone, and the other protocol is used between them. Zone Routing Protocol (ZRP) is the example of Hybrid Routing Protocol. ZRP uses proactive mechanism for route establishment within the nodes neighbourhood, and for communication amongst the neighbourhood it takes the advantage of reactive protocols. These local neighbourhood are known as zones, and the protocol is named for the same reason as zone routing protocol.

Reactive Protocols

Reactive protocols also known as on demand driven reactive protocols. The fact they are known as reactive protocols is, they do not initiate route discovery by themselves, until they are requested, when a source node request to find a route. These protocols setup routes when demanded. When a node wants to communicate with another node in the network, and the source node does not have a route to the node it wants to communicate with, reactive routing protocols will establish a route for the source to destination node. Normally reactive protocols.

- Don't find routeed until de
- When the protocol attempts to find the destination "on demand", it uses f propagate the query.
- Do not consume bandwidth for sending information.
- They consume bandwidth only, when the node start transmitting the data to the destination node.

Further Classification

Ad-Hoc on Demand Distance Vector Protocol (AODV)

AODV is a reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route. AODV will provide topology information for the node. AODV use control messages to find a route to the destination node in the network. There are three types of control messages in AODV which are discussed below.

Route Request Message (RREQ): Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

Route Reply Message (RREP): A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

Route Error Message (RERR): Every node in the network keeps monitoring the link status to its neighbour'snodesduring active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is a fault link.

Dynamic Source Routing Protocol

Dynamic source routing protocol abbreviated as DSR is also a reactive protocol. DSR use to update its route caches by finding new routes. It updates its cache with new route discovered or when there exist a direct route between source and destination node. When a node wants to transmit data, it defines a route for the transmission and then starts transmitting data through the defined route. There are two processes for route discovery and maintenance.

Route Discovery Srocess: When a source node wants to start data transmission with another node in the network, it checks its routing cache. When there is no route available to the destination in its cache or a route is expired, it broadcast RREQ. When the destination is located or any intermediate node that has fresh enough route to the destination node, RREP is generated. When the source node receives the RREP it updates its caches and the traffic is routed through the route.

Route Maintenance Process: When the transmission of data starts, it is the responsibility of the node that is transmitting data to confirm the next hop received the data along with source route. The node generates a route error message, if it does not receive any confirmation to the originator node. The originator node again performs new route discovery process.

Cooperative Bait Detection Scheme

Cooperative Bait Detection Scheme (CBDS), is used to detect and prevent malicious nodes which results in grayhole and blackhole attacks in MANETs. The source node selects an adjacent node and makes a cooperate connection with the respective node. So the address of this node is used as bait to trap the malicious nodes. Malicious nodes are thereby detected and prevented from participating in the routing operation. When there is a drop in the packets that are sent from source to destination, the destination node sends a signal informing about the packet loss to the source node to start the detection mechanism again. CBDS method uses both the proactive and reactive technique to detect the malicious node in the routing path. It first sends the RREQ signal and waits for the RREP signal. After receiving the signal it can identify all the addresses of nodes in the selected routing path from source to destination.

By using this address it cooperates with the nearby nodes and makes them as trust worthy nodes and finally the bait is set to trap the malicious nodes. After the detection of malicious nodes packets get transmitted through the unaffected path to avoid Blackhole and Grayhole attacks.

So this method detects the malicious nodes by using bait technique. Therefore the malicious nodes are prevented from participating in the data transfer operation thereby avoiding Blackhole and Grayhole attacks.

IMPLEMENTATION

Implementation is the methodology for detecting the attacks caused due to malicious nodes. It also implements the CBDS technique to detect the malicious nodes and thereby avoiding the attacks.

Modules

1. Network Formation
2. Include Hacker Node
3. CBDS
4. Update malicious node in Route Cache

Network Formation

Here, we have to create nodes. We select the source and destination. After selecting the source and destination, source wants to send the data to destination. So we need a route for data forwarding.

Include Hacker Node

After create a network, we have to include a hacker node. Hacker nodes always try to enter the network. Initially source will send Route Request. Destination node will send a Route Reply. But here Hacker node will send fake Route Reply to particular destination. Previous techniques able to check whether a Good route or fake route is. After joining the network it will start to lose the data.

CBDS

Collaborative Bait Detection Scheme, initially source will generate one bait RREQ, destination address should be a one hop neighbours address. That one hop neighbour must be co-operating with a sou send Route Reply. So when source node will receive the Route Reply. It will know some hacker node is available on the network.

Update malicious node in Route Cache

When hacker node found on the network, the node will update the hacker details from the route cache. In this scheme, we will use DSR protocol for routing.

RESULTS AND DISCUSSION

Simulation Results

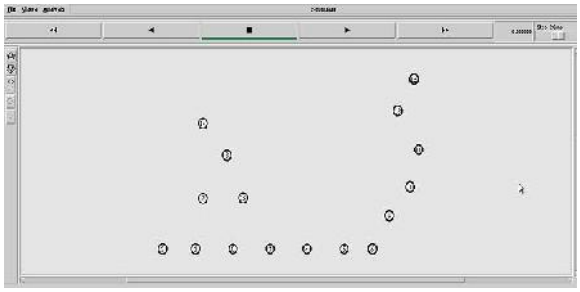
There are two types of outputs

- NAM window
- X graph

NAM Window

For determining the results first we select the required number of nodes the system. Here we select 15 nodes initially.

Figure 3: Total Nodes



The source node sends the route request (RREQ) message to all the nodes in the

Figure 4: Transmission of RREQ Signal

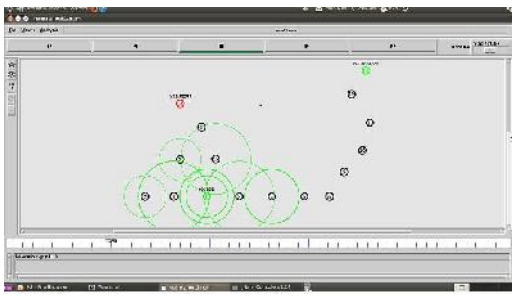
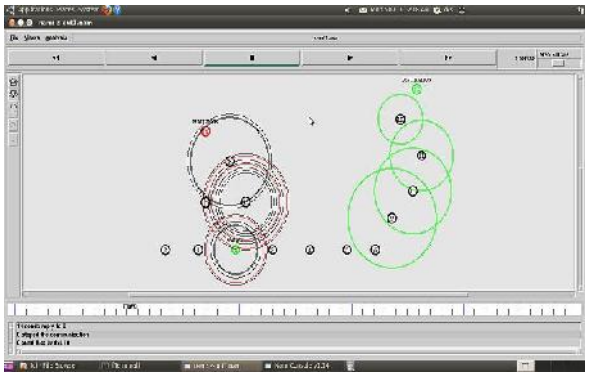


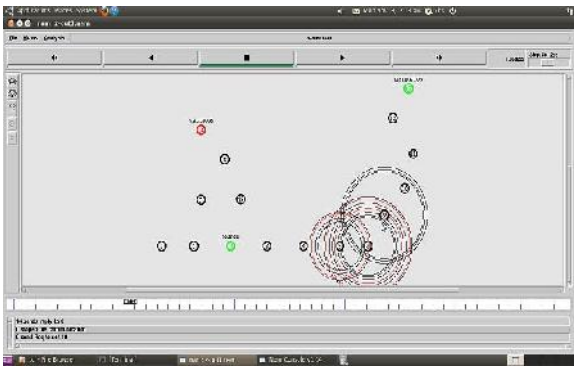
Figure 5: Reception of RREP Signal



system. It waits for the route reply message from all the nodes.

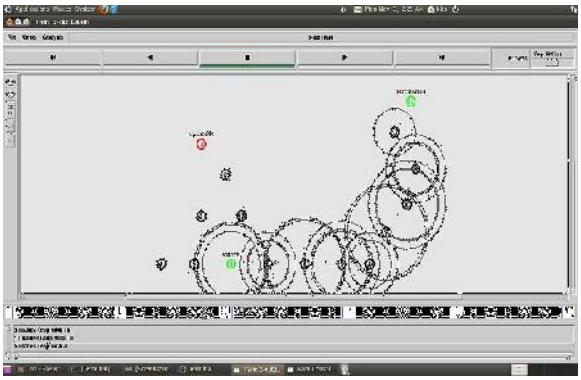
After detecting the malicious nodes in a route the source does not send the message through the route which has the malicious node. It then finds the alternate path for sending the message to the destination. It again sends the RREQ signal through the new path and waits for the RREP signal from the nodes which are in the selected path.

Figure 6: Reception of RREP Signal from Alternate Path



After finding the path which is free from malicious nodes, the source starts to send the data packets through this route for efficient data transmission without any packet loss.

Figure 7: Transmission of Packets from Source to Destination



X-GRAPH

Packet Delivery Fraction

PDF is defined as the ratio of the number of packets received at the destination and the number of packets sent by the source. The bottom line denotes represents the normal method values and the cone shaped line represents the Bait method values. Below diagram shows the number of packets that are delivered for respective time periods.

Routing Overhead

RO is the ratio of the amount of routing-related control packet transmissions to the amount of data transmissions. The bottom line denotes

Figure 8: PDF Comparison

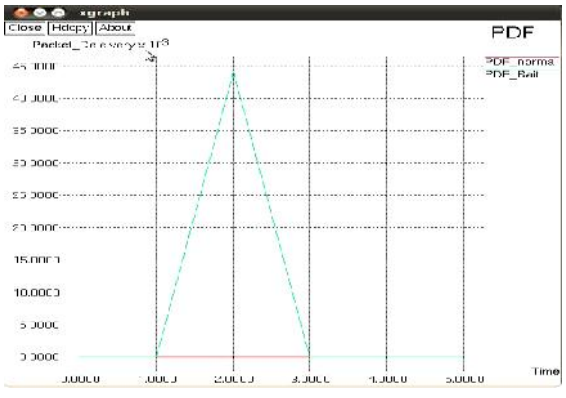
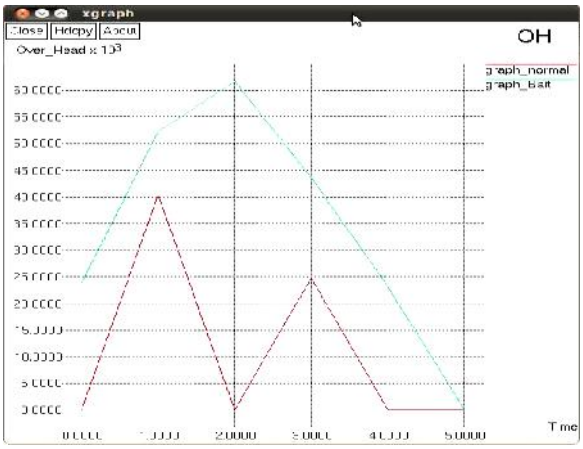


Figure 9: RO Comparison



the Normal method values and below diagrams shows the amount of packets delivered for respective time periods.

CONCLUSION

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. Here analysis is based on the behavior and challenges of security threats in mobile Ad-Hoc networks with solution finding technique.

Although many solutions have been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of single malicious node, it cannot be applicable in case of multiple malicious nodes. After studying all the approaches, our conclusion is that Enhanced CBDS approach overcomes the Blackhole and Grayhole attacks in an effective manner.

On further analysis the Enhanced CBDS method outperforms the existing schemes in terms of routing overhead and packet delivery ratio.

FUTURE WORK

Mobile Ad-Hoc networks are widely used networks due to their flexible nature i.e. easy to deploy regardless of geographic constraints. These networks are exposed to both external and internal attacks as there is not centralized security mechanism. So as future work, this project intends to investigate the integration of the CBDS with otherwell-known message security schemes in order to construct a comprehensive secure routing framework to protect MANETs against miscreants.

REFERENCES

1. Denis Dondi, Alessandro Bertacchini, David Brunelli, Luca Larcher and Luca Benini (2011), “Modeling and Optimization of a Solar Energy Harvester System for Self-Powered Wireless Sensor-32: Networks”, p. 28.
2. James Parker, Jeffrey Undercoffer, John Pinkston, and Anupam Joshi (2007), “On Intrusion Detection and Respon for Mobile Ad Hoc Networks”.
3. Jin-Shyan Lee (2010), “A Petri Net Design of Command Filters for Semiautonomous Mobile Sensor Networks”, pp. 255-265.
4. Kejun Liu, Jing Deng, Pramod K Varshney and Kashyap Balakrishnan (2009), “An Acknowledgment Approach for the Detection of Routing Misbehavior in MANETs”.

5. Lidong Zhou and Zygmunt Securing Ad J Haas (2011), "Hoc Networks", pp. 1-5.
6. Nidal Nasser and Yunfeng Ch, "Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks".
7. Yanchao Zhang, Wei Liu and Wenjing Lou (2002), "Anonymous Communications".
8. Ye Zhu, Xinwen Fu, Bryan Graham, Riccardo Bettati and Wei Zhao (2007), "On Flow Cor Measures in Mix Networks", Vol. 550, pp. 536.
9. Yih-Chun Hu, David B Johnson and Adrian Perrig (1999), "SEAD: SecureEfficient", Distance Vector Routing for Mobile Wireless".
10. Yunseop (James) Kim, Robert G Evans and William M Iversen (2011), "Sensing and Control", *Remotofan Irrigation System Using a Distributed Wi*.