ISSN: 0976-3104
SPECIAL ISSUE: Emerging Technologies in Networking and Security (ETNS)
Keerthika and Malarvizhi

ARTICLE OPEN ACCESS

IMPACT OF BLACK HOLE ATTACK UNDER DIFFERENT SCENARIOS ON AD HOC ON-DEMAND DISTANCE VECTOR

Keerthika[1] and Malarvizhi[2]
[1]*Veltech Dr.RR & Dr.SR Technical University, Avadi, Chennai, TN, INDIA*
[2]*Dept of CSE, Veltech Dr.RR & Dr.SR Technical University, Avadi, Chennai, TN, INDIA*

ABSTRACT

Mobile Ad hoc Networks (MANETs)are self-configuring networks with nodes being connected through wireless links forming a multi-hop radio network without infrastructure or administration. Security is a major issue in MANETs due to dynamically changing topologies, lack of centralized monitoring, open medium, and bandwidth constraints. It faces security issues not addressed by the security services of infrastructure based networks. Routing performance deteriorates in MANETs due attacks. Ad hoc On-demand Distance Vector (AODV) is a suitable MANET routing protocol that is highly vulnerable to black hole attack by malicious nodes. This study simulates/analyses the impact of black hole attack on an AODV protocol.

Published on: 28th– August-2016

KEY WORDS

Mobile Ad hoc Networks (MANETs), Ad hoc On-demand Distance Vector (AODV), Black Hole Attack.

***Corresponding author: Email:** keerthivenkatt@gmail.com; **Tel.:** +91-9790428279

INTRODUCTION

Mobile Ad hoc Networks (MANETs) are groups of independent mobile nodes communicating with each other through radio waves (wireless links). A node has a wireless interface to communicate and mobile nodes in radio range communicate directly whereas intermediate nodes are required to route packets to nodes beyond the radio range. Such networks are self-configuring, fully distributed, and work at any place without fixed infrastructure like access points/base stations [1].

MANETs have advantages over conventional networks including reduced infrastructure costs, easy establishment, and fault tolerance as routing is by individual nodes using intermediate network nodes for packet forwarding which reduces bottlenecks. The major MANET attraction is greater mobility compared to wired solutions. MANETs have dynamic topology with mobile nodes having limited resources like battery, processing power and onboard memory. Such infrastructure-less networks are used in situations where ordinary wired networks are infeasible including battlefields and natural calamities. Nodes within transmission range communicate directly or communication is via intermediate nodes which forward packets. Hence, these networks are called multi-hop networks.

Routing protocol design is a challenge due to ad hoc network's dynamism. Routing is an interesting MANET research area, which received tremendous attention from researchers. Guaranteeing delivery and ability to handle dynamic connectivity are important issues for wireless MANET routing protocols. When there is source to destination path for a specific time, routing protocols should deliver data through that path [2].

Routing protocols use metrics to calculate best path to route packets to destinations. Metrics are standard measurements that are number of hops used by a routing algorithm to determine the optimal path for a packet to reach a destination. Path determination process is that routing algorithms initialize/maintain routing tables with a packet's total route information [3].

THE IIOAB JOURNAL
ISSN: 0976-3104

Routing protocols define rules set, which govern the transmission of message packets from source to destination in networks. In MANETs, there are different routing protocols each used according to network circumstances. Routing protocols based on properties are classified as proactive, reactive and hybrid routing protocols [2].

MANET's dynamic environment's routing protocol security is a challenge. A self-organizing environment introduces security issues not addressed by security services meant for infrastructure based networks. Secure routing protocols deal with malicious nodes that disrupt routing protocol functioning by modifying routing information, fabricating routing information and impersonating nodes [4].

The first line of defence to reduce attacks are attack prevention measures like authentication and encryption. But, these do not suit MANET's resource constraints, i.e., limited bandwidth and battery power, as heavy traffic load emanates to exchange/verify keys.

MANET attacks are classified into passive and active attacks. A passive attack exchanges data in a network without disrupting communications while active attacks involve information interruption, modification/fabrication disrupting MANET functioning.

The attacks are divided into external and internal attacks, according to the attack domain. External attacks are mounted by nodes not belonging to a network whereas internal attacks are due to compromised nodes within the network. Internal attacks are more disruptive as an insider knows and can access confidential information. An attacker in external attacks causes congestion, propagates fake routing information or disturbs nodes from providing services. In internal attacks, an adversary participates in network activities, through impersonation as a new node, or by compromising a current node and using it as a conduit for its nefarious work.

AODV is a reactive routing protocol where routes are determined when required. It exchanges messages [5] and is used for unicast, broadcast, and multicast communication. It adopts basic Route Discovery and Route maintenance mechanism on demand from Dynamic Source Routing (DSR) and Destination Sequenced Distance Vector (DSDV) hop by hop routing sequence number and periodic beacons. This study discusses the impact of black hole attacks on MANETs with AODV routing protocol. Section 2 deals with literature related to this work, Section 3 reveals methods used in the work, Section 4 provides results and discussions of the obtained results, and Section 5 concludes the work.

LITERATURE REVIEW

Highlighting attack scenarios in multicast routing protocols that exploited vulnerabilities was attempted by Singal et al., [10]. Attacks were from a multicast routing protocols perspective were implemented. They analyzed blackhole , jellyfish drop, and neighbourhood attacks impact on ODMRP routing protocol for MANETs. Some techniques forwarded by researchers to detect and prevent black hole attack in MANETs using AODV protocol were discussed by Sarma et al., [11] and a new methodology based on their flaws was proposed. The effects of the attacks on applied AODV protocol based on performance metrics like throughput, packet drop ratio, normalized routing load, and dropped packets number on parameters like varying speed, nodes, and pause time was exhibited by Chadha and Jain [7]. A measure to reduce black hole attack was also analysed on metrics. A method against black hole attacks in MANETs presented by Narayanan and Radhakrishnan [13] used destination MAC address to validate a node in its path thereby ensuring a direct secure route. Simulation was carried out on the new scheme to prove the effectiveness of the mechanism in attack mitigation while maintaining a reasonable throughput, packet delivery ratio, and end to end delay.

A mechanism like trust based routing, intrusion detection system, sequence number comparison, and data routing information table to overcome black hole attack was proposed by Venkanna and Velusamy [8]. Trust based on-demand routing mechanism identifies and decreases hazards by malicious node on a path. A survey to prevent and identify black hole attack using trust management mechanism in MANET was undertaken. Serrat-Olmos et al., [9] proposed a collaborative approach to detect black holes and selfish MANET nodes, using a Bayesian watchdogs set, which enhanced individual/collective performance. Results revealed that misbehaved nodes detection time was reduced, and false positives and false negatives impact was minimised while overall accuracy increased. The results were confirmed by simulation. The collaborative Bayesian watchdog performed better than standard Bayesian watchdog regarding accuracy and quick detection.

Chaubey et al., [6] proposed a network size, Trust based Secure on Demand Routing Protocol (TSDRP) and AODV routing protocol secured it against black hole attack. AODV is a MANET routing protocol, without in-built security measures and so is vulnerable to attacks. Black hole attack at network layer is a major attack in this routing protocol. It considers average end-to-end delay average throughput, packet delivery fraction and normalized routing load to evaluate performance. Modification of AODV routing protocol was suggested by Wahane and Lonare [12]. A mechanism was used to detect and defend against cooperative black hole attacks. The authors suggested two concepts including Maintenance of Routing Information Table and second being node Reliability checking. This decreased end to end delay and Routing overhead.

Lu et al., [17] proposed and implemented Bad AODV (BAODV) Routing by simulating black hole attack in MANET. SAODV protocol based on BAODV, addressed AODV protocol's security weakness and withstood black hole attack. Analysis showed that SAODV was more secure than basic AODV.DOA and AODV routing protocols used in large scale networks were analysed by

THE IIOAB JOURNAL ISSN: 0976-3104

Jeni et al., [14] who used them in black hole attack and evaluated quality parameters like packet delivery ratio and average end to end delay. Sharma and Sharma [15] presented two solutions. The first was locating more than one destination route and the second was exploiting packet sequence numbers in packet headers. Simulation revealed that compared to the original AODV routing scheme, the second solution verified 75% to 98% destination routes depending on pause time with minimum network delay. The objective was to analyse black hole attack in a MANET and its solutions.

Thachiland Shet [16] presented a collaborative approach to mitigate black hole nodes in MANET's AODV protocol where a node monitors neighbouring nodes and calculates their trust value dynamically. When a monitored node's trust value is below a predefined threshold, then the monitoring node assumes it as malicious and avoids it. Experiments revealed that the new scheme mitigated black hole nodes and secured AODV routing protocol for MANETs. Conquering black and gray hole attacks was proposed by Yang et al., [18] whose watchdog mechanism based neighbour observed model detected one black hole attack by focusing on direct trust value. Historical evidence was considered against gray hole attacks. A neighbour recommendation model accompanied by indirect trust value figured out a cooperative black hole attack. Both revealed good results and proved the new method's advantages by punishing malicious actions to prevent attack camouflage/deception.

METHOD

This section discusses black hole attack's impact on MANETs with AODV routing protocol.

AD HOC ON-DEMAND DISTANCE VECTOR (AODV)

AODV routing protocol is a MANET routing protocol. AODV router is a state machine processing incoming requests from a network. When a network has to send a message to a node, it asks AODV to determine the next-hop [5].Though AODV uses DSDV sequence numbers and routing beacons it performs route discovery with on-demand Route Requests (RREQ) similar to DSR protocol. AODV uses sequence numbers to handle node mobility to identify/discard out-dated routes. Route Error (RERR) messages for detecting broken links. RERR packets travel to source informing nodes to delete broken links triggering new route discovery when alternative routes are unavailable.

AODV, unlike DSR is an on-demand, single path, loop-free distance vector protocol using source routing through a hop-by-hop routing approach. AODV is better than DSR for high mobility but has high routing load problems compared to DSR as the latter resorts to aggressive route caching which AODV does not. So, there are researches which solve AODV's problems using cache memory. AODV has DSDV's properties which include DSR's loop free properties using cache memory. A route is created on demand by a network connection in AODV and information regarding a route is stored in nodes routing tables on the route path [19].

AODV shares DSR's on-demand characteristics as it also discovers routes on demand by flooding networks with RREQ packets. A node, on receipt of an RREQ rebroadcasts it unless it is a destination or has a route to it in its cache. The node replies to RREQ with an RREP packet reverted back to the original source. AODV maintains routing information through conventional tables, one entry per destination.

AODV, relies on routing table entries to propagate RREP back to source without source routing and to route data packets to a destination. AODV uses sequence numbers in destinations to determine routing information freshness and to prevent routing loops. Maintenance of timer-based states in nodes is an important AODV feature, on use of individual routing table entries [20].

In AODV, routing updates through RREQs/RREPs are '*route advertisements*.' Update rules in **[Figure -1]** are invoked by nodes on receipt of route advertisements which help maintain loop freedom.

Consider the tuple $\left(-seq\_num_i^d, hop\_count_i^d\right)$ where $seq\_num_i^d$ represents the sequence number for destination *d* at node *i*, and $hop\_count_i^d$ represents the hop count from node *I* to destination *d*.

Define $\left(-seq\_num_i^d, hop\_count_i^d\right) > \left(-seq\_num_j^d, hop\_count_j^d\right)$ if and only if either $seq\_num_i^d < seq\_num_j^d$, or $seq\_num_i^d = seq\_num_j^d$ and $hop\_count_i^d > hop\_count_j^d$ (i.e., lexicographic ordering among $\left(-seq\_num_i^d, hop\_count_i^d\right)$ tuples).

A node *i*applies these rules on receipt of a route advertisement for destination *d* from a neighbour *j*. Variables $seq\_num_i^d$, $hop\_count_i^d$, and $next\_hop_i^d$ denote destination sequence number, hop count and next hop respectively for destination *d* at node *i*.

THE IIOAB JOURNAL
ISSN: 0976-3104

1: **if** $\left(\text{seq\_num}_i^d < \text{seq\_num}_j^d\right)$ **or** $\left(\left(\text{seq\_num}_i^d = \text{seq\_num}_j^d\right)$ **and** $\left(\text{hop\_count}_i^d > \text{hop\_count}_j^d\right)\right)$ **then**

2: $\text{seq\_num}_i^d := \text{seq\_num}_j^d$;

3: $\text{hop\_count}_i^d := \text{hop\_count}_j^d + 1$;

4: $\text{next\_hop}_i^d := j$;

5: **end if**

Fig:1. AODV route update rules

BLACK HOLE ATTACK

Black hole attack is a Denial of Service (DoS) attack in MANETs where a malicious node advertises about a best path it has to a destination node during route discovery. When it receives a RREQ message, it sends a fake RREP to source node immediately. The source node receives the RREP from the malicious node before other RREPs. But, when the source node starts sending data packet to the destination using the given route, the malicious node drops packets instead of forwarding [21] them.

A black hole problem is seen in **[Figure -2]**, where node "A" asks node "D" to send data packets and starts discovering a path. So, if node "C" is a malicious node, it claims it has a positive route to a specific destination, till the road receiving a request (RREQ) packet is open. It responds to node "A" through any node. Thus, node "A", ie; on the path takes a positive discovery initiative. Node "A" ignores other responses and plants package node "C". So, all lost packets are consumed/lost.

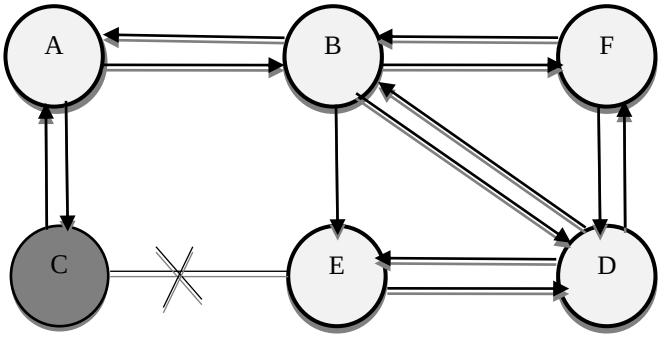

Fig: 2. Black hole attack in AODV

Detection is complicated in MANETs due to limited resources like bandwidth, battery life, and storage. Concerns about minimum possible rise in routing overhead and end-to-end delay affect implementing any detection process. Related research implemented detection method against AODV routing through Dynamic Learning Method[22].

An attacker sends fake RREQ messages to form black holes. In a RREQ black hole attack, an attacker pretends to rebroadcast a RREQ message with a non-existent node address. Other nodes update their route to bypass non-existent node to the destination node. The attacker forms a black hole between source and destination nodes through a fake RREQ message.

RESULT AND DISCUSSION

Network simulation was through NS2, and the performances of AODV were compared for non-malicious and malicious network. Simulations are conducted with number of nodes that 30, 60, 90, 120 and 150. The nodes are spread over an area of 4000 sqm and has a transmission range of 200 m. Traffic transmitted are in Constant Bit Rate (CBR). The impact of AODV without malicious nodes, with 15% malicious node, with 30% malicious node and with 45% malicious node. The simulation parameters are summarized in **[Table- 1].**The results achieved for packet delivery ratio, average end to end delay and number hops to sink are presented in this section.

THE IIOAB JOURNAL
ISSN: 0976-3104

Table: 1. Simulation Parameters

Parameter	Value
Number of Nodes	30, 60, 90, 120 and 150
Network area	4000 m^2
Transmission range	200 m
Traffic	CBR
Routing	AODV
Maliciousness	15%, 30% and 45% maliciousness

Table: 2. Average End to End Delay in second

Number of nodes	AODV without malicious nodes	AODV with 15%malicious	AODV with 30% malicious node	AODV with 45% malicious node
30	0.00086	0.00109	0.00131	0.0013
60	0.00107	0.00129	0.00173	0.00152
90	0.0013	0.00281	0.00356	0.00173
120	0.00129	0.0042	0.00534	0.00182
150	0.00794	0.01287	0.01639	0.01093

It can be observed from **[Table -2]** that the maliciousness in network tends to increase the end to end delay. It is observed from the simulation results that the end to end delay increases by 28.38% to 40.74% for a 45% malicious network.

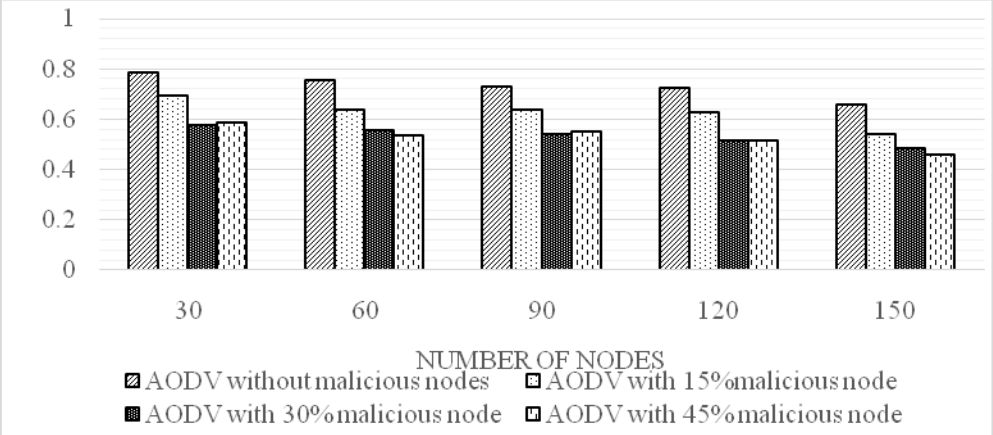

Fig: 3.Packet Delivery Ratio

It can be observed from **[Figure -3]** that the packet delivery ratio decreases with increase in number of nodes and increase in maliciousness in the network. The packet delivery ratio ranges from 0.66 to 0.79 for AODV without maliciousness in the network. As the maliciousness increases the delivery ratio decreases drastically. For a network with 15% maliciousness, the packet delivery ratio decreases in the range of 12.36% to 19.6%.

THE IIOAB JOURNAL
ISSN: 0976-3104

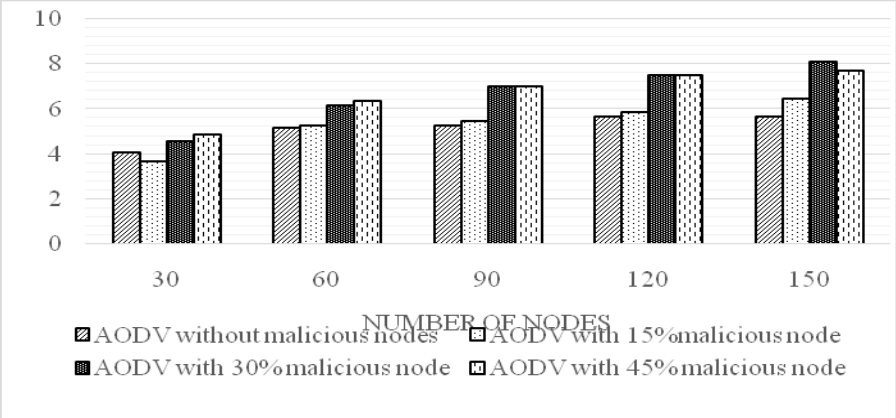

Fig: 4. Average Number of hops to sink

It can be observed from **[Figure -4]** that the number of hops increases as the maliciousness in the network increases.

CONCLUSION

This study analysed the effect of black hole attack in AODV protocol performance. Metrics like packet delivery ratio, average end to end delay in second and average hops to sink were evaluated and analysed with variable node mobility, number of nodes. Simulation shows that when black hole node exists in a network, it can affect and decrease performance of AODV routing protocol. So black hole attack detection and prevention in a network is a challenge. Future direction of work to create a solution for black hole attack and to compare its performance with AODV

CONFLICT OF INTEREST

Authors declare no conflict of interest.

ACKNOWLEDGEMENT

None

FINANCIAL DISCLOSURE

No financial support was received to carry out this project.

REFERENCES

[1] Aarti DS. [2013] Tyagi,Study Of Manet: Characteristics, Challenges, Application And Security Attacks". *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(5):252-257.

[2] Rhee I, Shin M, Hong S, Lee K, Kim SJ, Chong S. [2011] On the levy-walk nature of human mobility. *IEEE/ACM transactions on networking (TON)*, 19(3): 630-643.

[3] Gorantala K. [2006] Routing protocols in mobile ad-hoc networks. *A Master'thesis in computer science,* -1-36.

[4] Zhang D, Gogi SA, Broyles DS, Çetinkaya EK, Sterbenz JP. [2012] Modelling wireless challenges. In *Proceedings of the 18th annual international conference on Mobile computing and networking*, ACM, 423-426.

[5] Chakeres ID, Belding-Royer EM. [2004] AODV routing protocol implementation design. In Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on , *IEEE*, (pp. 698-703)

[6] Chaubey N, Aggarwal A, Gandhi S, Jani KA. [2015] Performance Analysis of TSDRP and AODV Routing Protocol under Black Hole Attacks in MANETs by Varying Network Size. In *Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on*(pp. 320-324). *IEEE*.

[7] Chadha K, Jain S. [2014] Impact of black hole and grayhole attack in AODV protocol. In *Recent Advances and Innovations in Engineering (ICRAIE), 2014* (pp. 1-7). *IEEE*.

[8] Venkanna U, Velusamy RL. [2011] Black hole attack and their counter measure based on trust management in manet: A survey. In *Advances in Recent Technologies in Communication and Computing (ARTCom 2011), 3rd International Conference on* (pp. 232-236). *IET*.

[9] Serrat-Olmos MD, Hernández-Orallo E, Cano JC, Calafate CT, Manzoni P. [2012] Accurate detection of black holes in MANETs using collaborative bayesian watchdogs. In *Wireless Days (WD), 2012 IFIP* (pp. 1-6). *IEEE*.

[10] Singal G, Garg H, Laxmi V, Gaur MS, Lai C. [2014] Impact analysis of attacks in multicast routing algorithms in MANETs.

THE IIOAB JOURNAL ISSN: 0976-3104

InIndustrial and Information Systems (ICIIS), 2014 9th International Conference on (pp. 1-6). *IEEE*.

[11] Sarma KJ, Sharma R, Das R. [2014] A survey of Black hole attack detection in Manet. In *Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on* (pp. 202-205). *IEEE*.

[12] Wahane G, Lonare S. [2013] Technique for detection of cooperative black hole attack in MANET. In *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)* (pp. 1-8). *IEEE*.

[13] Narayanan SS, Radhakrishnan S. [2013] Secure AODV to combat black hole attack in MANET. In *Recent Trends in Information Technology (ICRTIT), 2013 International Conference on* (pp. 447-452). *IEEE*.

[14] Jeni PJ, Vimala Juliet A, Parthasarathy R, Messiah Bose A.[2013] Performance analysis of DOA and AODV routing protocols with black hole attack in MANET. In *Smart Structures and Systems (ICSSS), 2013 IEEE International Conference on* (pp. 178-182). IEEE.

[19] Al-jubori MJ, Pawale SS, Shinde SR. [2011]Efficient Ad-Hoc On-demand Distance Vector Routing Protocol using Link State Algorithm .*International Journal of Computer Applications*, 26(2).

[20] Barua G, Agarwal M. [2002] Caching of routes in ad hoc on-demand distance vector routing for mobile ad hoc networks. In *proceedings of the international conference on computer communication*, 15(2): 768

[21] Chaudhary A, Malhotra P. [2014] Impact of Black Hole Attack on AODV Routing Protocol. In *International Journal of Engineering Development and Research*, *IJEDR* 2(3) .

[22] Khandelwal V, Goyal D. [2013] BlackHole Attack and Detection Method for AODV Routing Protocol in MANETs. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *2*(4):1555.

[15] Sharma N, Sharma A. [2012] The black-hole node attack in MANET. In *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on* (pp. 546-550). IEEE.

[16] Thachil F, Shet KC. [2012] A trust based approach for AODV protocol to mitigate black hole attack in MANET. In *Computing Sciences (ICCS), 2012 International Conference on* (pp. 281-285). IEEE.

[17] Lu S, Li L, Lam K.Y, Jia L. [2009] SAODV: a MANET routing protocol that can withstand black hole attack. In *Computational Intelligence and Security, 2009. CIS'09. International Conference on , IEEE*, 2:421-425.

[18] Yang B, Yamamoto R, Tanaka Y. [2014] Dempster-Shafer evidence theory based trust management strategy against cooperative black hole attacks and gray hole attacks in MANETs. In *Advanced Communication Technology (ICACT), 2014 16th International Conference on* (pp. 223-232). *IEEE*.