I.J. Intelligent Systems and Applications, **2014, 06, 72-78**
Published Online May 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijisa.2014.06.08

Impact of Multipath Routing on WSN Security Attacks

Koffka Khan
Dept. of Computing and Information Technology, The University Of The West Indies, Trinidad, W.I.
E-mail: koffka.khan@sta.uwi.edu

Wayne Goodridge
Dept. of Computing and Information Technology, The University Of The West Indies, Trinidad, W.I.
E-mail: wayne.goodridge@sta.uwi.edu

Abstract— Multipath routing does not minimize the consequences of security attacks. Due to this many WSNs are still in danger of most security attacks even when multipath routing is used. In critical situations, for example, in military and health applications this may lead to undesired, harmful and disastrous effects. These applications need to get their data communicated efficiently and in a secure manner. In this paper, we show the results of a series of security attacks on a multipath extension to the ad hoc on-demand distance vector AODV protocol, AOMDV. It is proved that many security parameters are negatively affected by security attacks on AOMDV, which is contradictory to research claims. This means that alternative refinements have to be made to present multipath routing protocols in order to make them more effective against network security attacks.

Index Terms— multipath, wireless sensor networks, security attacks, AODV, AOMDV.

I. INTRODUCTION

In the context of wireless data communication, routing is of pivotal importance in getting information from one node to another. Getting information from one place in a wireless sensor network, usually from the data collecting nodes or source to the base station or sink is the primary objective. However, in military and medical applications [13], just getting the data across the network is not the only desired focus. In these applications security is of utmost importance due to the sensitive nature of the data that is transported. Hence, information security measures must be placed in these types of WSNs.

Multipath routing was initially designed to accommodate network failures, where allowing multiple ways to transport data across the network ensured no break in data transfer during path, node, environmental failures etc. A multipath routing algorithm is used to find the maximal number of paths between a single source-destination pair. Multipath routing aims to take advantage of the connectivity redundancies of the underlying physical networks by providing multiple paths between source-destination pairs [11]. However, this technique has its drawbacks, for example, excessive use of bandwidth, use of extra computing resources to eliminated duplicate messages, increased latency, message delays etc. Most WSN source routing protocols, for example, dynamic source routing (DSR) [4] and ad hoc on-demand distance vector (AODV) [10], [6] have a multipath variant, multimedia multipath dynamic source routing (MMDSR) [2] and ad hoc on-demand multipath distance vector protocol (AOMDV) [18], [1]. The route discovery process in the multipath protocols may be initiated either when the active path collapses where further communication is performed with one of the alternative paths, or when all known paths towards the destination are broken [20], known as complete multipath routing. The route discovery may stop when a sufficient number of paths are discovered or when all possible paths are detected. Multipath routing protocols can be node-disjoint [12] or link-disjoint [14] if a node (or a link) cannot participate in more than one path between two end nodes.

Inherently multipath routing protocols were not designed with security as a primary objective. However, some authors [7] argue that security mechanisms are not needed in multipath routing protocols because the use of many paths overcome the ‘majority’ of security issues faced by wireless sensor networks (WSNs). Recently, multipath routing algorithms have been introduced to enhance data confidentiality in ad hoc wireless networks [19], [3], [21], [17]. Intuitively, multipath routing algorithms are simple and efficient because no encryption is needed and data is “split” among different routes to minimize or even disable potential captures by unauthorized users [23]. Multipath routing minimizes the consequences of security attacks deriving from collaborating malicious nodes in MANET, by maximizing the number of nodes that an adversary must compromise in order to take control of the communication [16]. I would argue that even though this may be the case, security awareness still has to be built into such protocols in order for them to obtain the full benefit of transporting data from the source to the destination node. Further, the concept of multipath is refined in that even though a source can use multiple paths to get data to the desired destination, only one is actually used at any given point in time. From a security standpoint this means that only one alternative path is selected and used when a network layer security attack occurs.

The routing protocols have to be energy and memory efficient but at the same time they have to be robust to security attacks and node failures. From this perspective, eight WSN security parameters, availability, reliability, integrity, accessibility, survivability, responsiveness, self-healingness and resilience [7] are deemed as being important in the context of WSNs. These parameters define the security level of the WSN. They are defined by network performance measures and are indicative as to the overall security 'health' or 'well-being' of the WSN. Hence, a security threat is defined whenever one of these parameters is affected negatively.

This work focuses on the performance of the AOMDV routing protocol when exposed to security threats for WSNs. The outline of this paper is as follows. In section 2, wireless sensor network-based security parameters are presented. In section 3, AODV is introduced and explained together with its multipath extension AOMDV. Section 4 gives the experimental setup and simulations of the proposed methodology, while finally section 4 gives the advantages and disadvantages of using SA-AOMDV, with the conclusions.

II. Wireless Sensor Network-Based Security Parameters

The following security parameters can be used for measuring security attacks in WSNs:

1. *Availability-reliability-resiliency-self-healing:*

These WSN security parameters are given as the most important security requirements in critical WSN applications [7]. Availability ensures that services and information can be accessed at the time they are required. Reliability guarantees that data will be delivered to the destination, even in the face of threats. Resiliency ensures that the network will tolerate attacks while continuing to offer uninterrupted services. Self-healing deals with the ability to recover from security problems and isolate the source of the threat, ensuring continued availability.

2. *Integrity and freshness of data:*

These parameters verify that the data has not been altered maliciously while freshness deals with the fact that the data is up-to-date. Is source nodes send inaccurate data to the sinks then erroneous and harmful decision making will result, especially in sensitive applications, such as, health care and pollution monitoring, which relies heavily on the integrity and freshness of the information sent to them.

3. *Authentication:*

Authentication verifies the identity of the participants in WSN mote communication. Hence intruders can be distinguished from legitimate nodes. We place authentication third on the security requirements list as even if data is availability, integrity and freshness, we need to be sure that the trusted node has seen the packet and it has come from the node who has claimed to send it. It protects the network from malicious nodes who may inject false data into the network.

The methods used to evaluate network security metric parameter performance during a network attack are listed in Table 1.

Table 1. Security evaluation metrics

Metric	Measure
Availability	Blocked nodes
Reliability	Packet delivery
Integrity	Packet delivery
Accessibility	Blocked nodes, node density
Survivability	Energy consumption, routing overhead, retransmissions, path length
Responsiveness	Packet delivery delay
Self-healingness	Blocked nodes, routing overhead, retransmissions, packet delivery
Resilience	Eavesdropped packets, Blocked nodes, packet delivery, packet loss

III. Ad Hoc On-Demand Distance Vector Multipath Routing Protocol

A. *AODV*

The Ad hoc On-Demand Distance Vector (AODV) routing protocol is intended for use by nodes in an ad hoc network. AODV is a Reactive or on Demand routing protocol. It uses bi-directional links and a Route discovery cycle is used for route finding. There is also a route Maintenance phase of active routes. Sequence numbers are used for loop prevention and as an indicator for route freshness criteria. AODV provides unicast and multicast communication. AODV utilizes routing tables to store routing information. Typically a node stores a routing table for unicast routes and a routing table for multicast routes.

For each destination, a node maintains a list of precursor nodes, to route through them. Precursor nodes help in route maintenance. When a node wishes to send a packet to some destination it checks its routing table to determine if it has a current route to the destination. If it does, the node forwards the packet, via broadcast flooding, to next hop node. If not, it initiates a route discovery process. Route discovery process begins with the creation of a Route Request (RREQ) packet. Once an intermediate node receives a RREQ, the node sets up a reverse route entry for the source node in its route table.

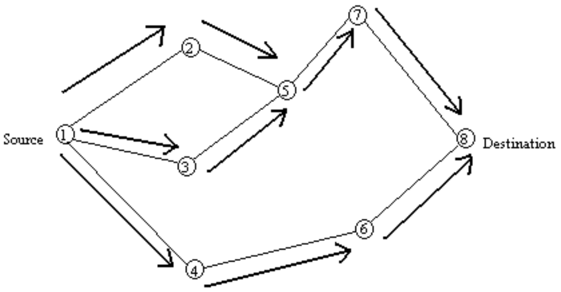

Fig. 1. Propagation of Route Request (RREQ) Packet

After the destination node receives the RREQ packet, using the reverse route a node can send a RREP (Route Reply packet) to the source. In order to respond to RREQ a node should have in its route table, (1) unexpired entry for the destination and (2) sequence number of destination at least as great as in RREQ (for loop prevention). If both conditions are met and the IP address of the destination matches with that in RREQ, the node responds to RREQ by sending a RREP back using unicasting and not flooding to the source using reverse path. If conditions are not satisfied, then source node increments the hop count in RREQ and broadcasts to its neighbours. After processing the RREP, the node forwards it towards the source.

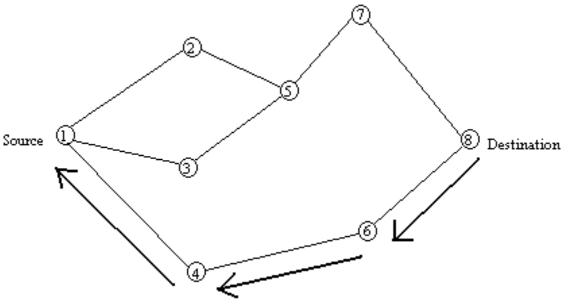

Fig. 2. Path taken by the Route Reply (RREP) Packet

Route Error (RERR) is initiated by the node upstream (closer to the source) of the break. It is propagated to all the affected destinations. RERR lists all the nodes affected by the link failure, that is, nodes that were using the link to route messages (precursor nodes). When a node receives an RERR, it marks its route to the destination as invalid by setting the distance to the destination as infinity in the route table. When a source node receives a RRER, it can reinitiate the route discovery. Link failure detection is enabled with Hello messages, where neighboring nodes periodically exchange hello message. Therefore, the absence of hello message is used as an indication of link failure. Alternatively, failure to receive several MAC-level acknowledgements may be used as an indication of link failure.

B. *AOMDV*

AOMDV is a multipath routing protocol. It is an extension to AODV and also provides two main services i.e. route discovery and maintenance. Unlike AODV, every RREP is being considered by the source node and thus multiple paths discovered in one route discovery. Being the hop-by-hop routing protocol, the intermediate nodes maintain multiple path entries in their respective routing table. The route entry table at each node also contains a list of next hop along with the corresponding hop counts. Every node maintains an advertised hop count for the destination. Route advertisements of the destination are sent using this hop count. An alternate path to the destination is accepted by a node if the hop count is less than the advertised hop count for the destination.

AOMDV provide all intermediate nodes in the primary route with alternative paths. Thus, when the route is broken, the intermediate nodes can be rescued by alternative paths. There is one common feature in most existing multipath routing protocols—among all routes, one is for use and the others are in the waiting list. When the current route is broken, another one is chosen to be the route from the waiting list.

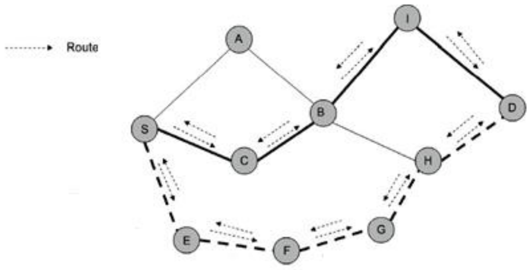

Fig. 3. AOMDV route discovery

Figure 4 shows how AOMDV will react to a network security attack. In this case when node G is compromised, AOMDV will continue sending data along route S-C-B-I-D.

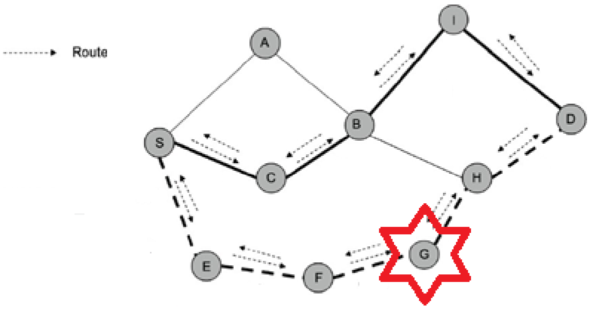

Fig. 4. AOMDV security attack (route selection at node S enables the new route S:C:B:I:D to be used for further communication)

IV. Simulation Results and Analysis

To evaluate the AOMDV routing protocol, we used the ns-2 simulator. The ns-2 simulator has been used extensively in evaluating the performance of ad hoc network routing protocols. These simulations model radio propagation using the realistic two-ray ground reflection model [5] and account for physical phenomena such as signal strength, propagation delay, capture effect, and interference. The Medium Access Control protocol used is the IEEE 802.11 Distributed Coordination Function (DCF) [9].

Table 2. Simulation settings

Method	Value
Simulator	Ns2.34
Environment	centOS
Channel type	Channel/WirelessChannel
Radio-propagation model	Propagation/TwoRayGround
Network interface type	Phy/WirelessPhy
MAC type	Mac/802.11
RTSThreshold	3000
Basic Rate	1Mb
Data Rate/Channel Bandwidth	2Mbps
Interface queue type	Queue/DropTail/PriQueue
Link layer type	LL
Antenna	Antenna/OmniAntenna
Maximum packet in ifq	50
Area (mxm)	500 x 500
Number of mobile nodes	8
Source type	UDP
Simulation time	80 sec
Routing protocol	AODV, AOMDV
Transmission range	250 m
Traffic generator	CBR
CBR rate	200 Kbits/s
Packet size/data payload	512 bytes
Transport protocol	UDP
Simulation time	80 econds

A. Evaluation Metrics

The following WSN performance evaluation parameters were used:

1. Throughput:

The throughput capacity is the number of bits per second that can be transmitted by every node to its destination. [1]

2. Delay:

The delay of a packet in a network is the time it takes the packet to reach the destination after it leaves the source. We do not take queueing delay at the source into account, since our interest is in the network delay. [1]

3. Packet loss:

The *Type-P-One-way-Packet-Loss* from Source to Destination at T is 1<< means that the Source sent the first bit of a type-P packet to Destination at wire-time T and that Destination did not receive that packet. [8]

B. Blackhole attacks

This attack is prevalent in WSNs and because it drops all packets destined for a particular destination is termed a blackhole attack. A blackhole attack occurs when a mote (internal blackhole) that is within the topology of the WSN or an outsider mote (external blackhole) inserts itself with a route to the sink that advertises itself as having the most lucrative to neighbourhood motes in forwarding their data packets to the destination mote. It does this by advertising itself to neighbours with the highest sequence number and lowest hop count. In this way neighboring motes are spoofed into believing that the blackhole mote offers a better path to the destination. They subsequently send their packets to the blackhole mote which drop all data packets. The mote establishes itself during the route discovery phase, by replying to RREQ messages with false RREP messages, with high sequence numbers and the lowest hop count to the destination mote. During data transmission the blackhole attack drops all data packets; hence the source mote and the destination mote are unable to communicate with each other.

In on-demand WSN routing protocols, blackhole attacks may target the route discovery phase. During route setup the rogue mote advertises a higher quality route to the sink compared to the other motes in its neighbourhood. It will do this by placing a lower hop count value in the route reply (RREP) packet destined to the source mote. The result will be that the source mote will be spoofed into believing that the blackhole mote has the best path to the desired destination. In all further communication to this destination mote, data packets will be sent via the blackhole mote. The blackhole mote acts by discarding all received packets. In single path routing protocols, where there may be many route discovery calls, compared to multi-path routing protocols, the blackhole attack may be more prevalent as there are more opportunities for the attacker to assert itself during the route discovery phase.

C. Simulation results

The network is configured with four sinks. Network attacks occur at 20-25s, 50-5s and 65-74s. Shown on the graphs are the output metric results for each of the sinks.

Throughput:

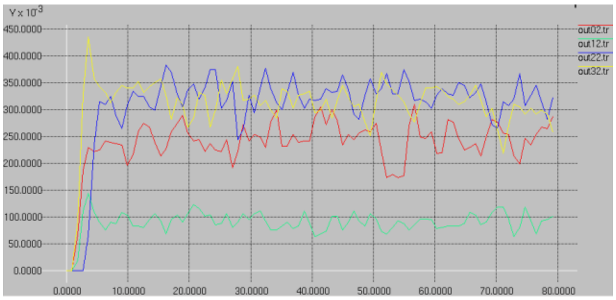

Fig. 6. AOMDV without network security breaches

Shown on Figure 6, for each sink the throughput was relatively stable with a peak of 425 Kbits/s obtained by sink 4 and a minimum of 60 Kbits/s in sink 2. The average throughput is approximately 225 Kbits/s.

Figure 7 shows the same network simulation but in this case there are three security attacks. The first has a duration of five seconds, the second attack has a duration of one second and the last had a duration of nine seconds. As seen the troughs in the graphs shows severe drops in throughput during the attacks. The effect on the network was so disastrous that in attacks lasting than more than one second, no data packets were transferred. In the case where the attack lasted one second, the throughput dropped from 200 Kbits/s to 145 Kbits/s. This is still a severe drop in throughput.

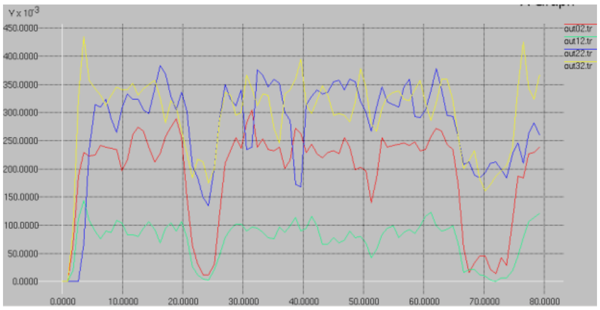

Fig. 7. AOMDV with network attacks

Delay:

Figure 8 shows the minimum delay was 18s with a maximum delay of 44s. The average delay was around 30s. The graph shows that the time taken for network data packets to traverse the network was relatively stable. The minor changes in delay could be attributed to changes in wireless network conditions.

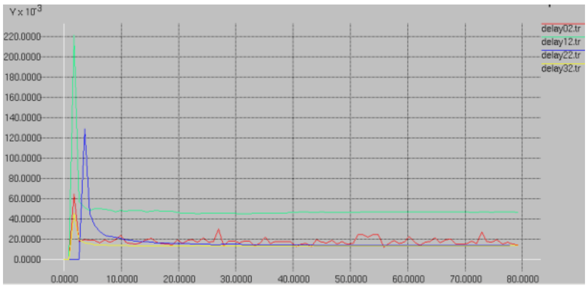

Fig. 8. AOMDV delay without network security breaches

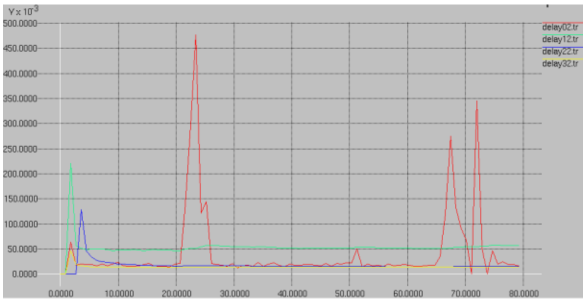

Fig. 9. AOMDV delay with network attacks

When the network is under attack maximum delay of 475s were found (cf. Figure 9). For short attacks, for example, the one lasting one second the delay went from 27s to 50s. For the delay lasting five seconds the maximum delay was found peaking at 475s from 25s. For the longest attack lasting nine seconds the peak delay was 347s.

Packet loss:

On Figure 10 is shown that the minimum packet losses were 20 packets, while the maximum packet losses were 210 packets. The average packet loss was around 85 packets. In a wireless environment the packet losses were as expected, varying according to network conditions.

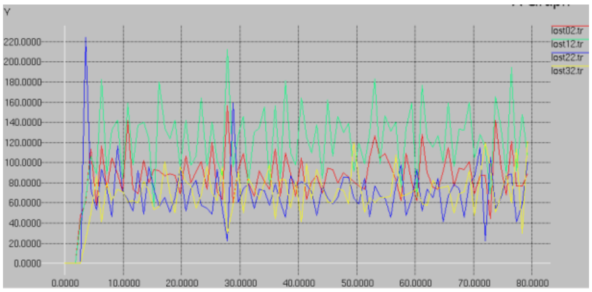

Fig. 10. AOMDV packet loss without network security breaches

Figure 11 shows that packet losses were consistent with that shown in Figure 10, except for three spikes. These spikes occurred just after the network was attacked. The first spike corresponded to the five second network attack and 750 packets were lost, whereas in the one second attack, a spike of 250 packets was observed. Finally for the nine second attack, a packet loss of 800 packets was seen.

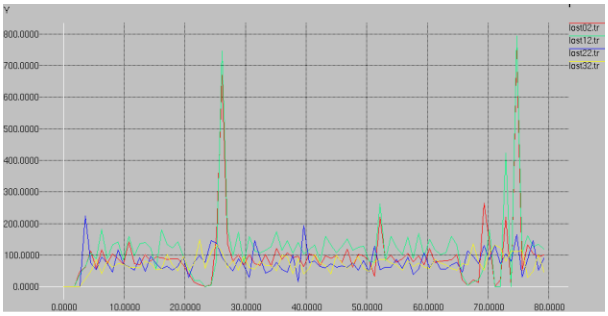

Fig. 11. AOMDV packet loss with network attacks

D. Discussions

The negative effects of security attacks on network performance parameters shows that multipath routing alone is not enough to protect a WSN. The network throughput is severely affected and this means that the security measure availability is breached. In situations where high performance is required this can be a very unsatisfactory outcome. Even though there are many different paths carrying the data packets, an attack shows that when one path is down the actual throughput to the sink drops and this finding does not support the argument that availability is unaffected by using a multipath protocol. It shows that even though data packets are still delivered to the host, most are dropped when an attack occurs. Hence, availability is severely affected.

Delay sensitive applications will be affected by security attacks in multipath environment. The literature states that delay should lessen under a security attack, when using a multipath protocol. A longer path may be under attack, hence when a network is under attack the shorter paths will get used, hence reducing the overall network delay. The results show that the delay increases when a network attack occurs. This happens as longer paths get selected, hence the delay would increase. Of course, the delay would depend on the ratio of longer to shorter path and if this is used as a routing metric. The delay would be determined by when the network is attacked, depending on if the attack is on a short path or longer path and if the switching is to a longer or shorter path. To the authors knowledge very little work has been done in this area, but primary results indicate that delay increases in multipath environments under attack.

Packet loss is fairly consistent for the cases of normal and 'under attack' network conditions. However, the large increases in packet losses just after an attack can be attributed to the switching to shorter more efficient paths after the attack. When this is done there is a natural loss of data packets in the network.

V. Conclusion

The authors show that research findings about the added security of multipath routing may be a myth. This is shown by a set of empirical simulated testing. The AOMDV routing protocol was used for testing in a WSN. The results show that network throughput and delay were negatively affected by network attacks, while packet loss remained fairly unaffected. The high importance of throughput and delay in resource intensive WSN applications means that immediate measures must be put into place for proper security mechanisms to be implemented in multipath routing protocols. This would enhance the use of such applications making them more effective, efficient and security-aware.

Acknowledgments

The authors would like to thank the anonymous reviewers for their careful reading of this paper and for their helpful comments. This work was supported by the National High Technology Research and Development Program of China under grant no. 2006AA060101.

References

[1] A. Gamal, J. Mammen, B. Prabhakar, D. Shah. Throughput-delay trade-off in wireless networks. In INFOCOM. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, 2004, (Vol. 1).

[2] C. Fr ás, D. D áz, A. Zavala, I. Aguilar. Dynamic cross-layer framework to provide QoS for video streaming services over ad hoc networks, 2012.

[3] C. K.-L. Lee, X.-H. Lin, and Y.-K. Kwok, "A Multipath Ad Hoc Routing Approach to Combat Wireless Link Insecurity," Proc. ICC 2003, vol. 1, pp. 448–452, May 2003.

[4] D. Johnson, D. Maltz. Dynamic source routing in ad hoc wireless networks. Mobile computing, 1996, pp. 153-181.

[5] D. Kotz, et al. "Experimental evaluation of wireless simulation assumptions." Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems. ACM, 2004.

[6] E. Royer, C. Perkins, An implementation study of the AODV routing protocol. In IEEE Wireless Communications and Networking Confernce, 2000, (Vol. 3, pp. 1003-1008).

[7] E. Stavrou, A. Pitsillides. A survey on secure multipath routing protocols in WSNs. Computer Networks, 2010, 54(13), 2215-2238.

[8] G. Almes, S. Kalidindi, M. Zekauskas. A one-way packet loss metric for IPPM. RFC 2680, 1999..

[9] G. Bianchi. "Performance analysis of the IEEE 802.11 distributed coordination function." *Selected Areas in Communications, IEEE Journal, 2000,* 18.3: 535-547.

[10] I. Chakeres, E. Belding-Royer. AODV routing protocol implementation design. In IEEE Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference, 2004, pp. 698-703.

[11] J. Chen, "New approaches to routing for large-scale data networks", Ph.D dissertation, Rice university, 1999.

[12] J. Wu. An extended dynamic source routing scheme in ad hoc wireless networks. Telecommunication Systems, 22(1-4):61–75, 2003.

[13] M. Hussain, K. Kyung. WSN research activities for military application. In Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference, 2009, (Vol. 1, pp. 271-274). IEEE.

[14] M. K. Marina and S. R. Das. Ad hoc on-demand multipath distance vector routing. ACM SIGMOBILE Mobile Computing and Communications Review, 2002, 6(3).

[15] P. Gupta, P. Kumar. The capacity of wireless networks.Information Theory, IEEE Transactions on, 2000, 46(2), 388-404.

[16] P. Kotzanikolaou, R. Mavropodi, R. C. Douligeris. Secure multipath routing for mobile ad hoc networks. In IEEE *Wireless On-demand Network Systems and Services, 2005. WONS 2005. Second Annual Conference, 2005,* (pp. 89-96).

[17] P. Papadimitratos and Z. J. Haas, "Secure Data Transmission in Mobile Ad Hoc Networks," Proc. ACM WiSe 2003, pp. 41–50, Sept. 2003.

[18] P. Sambasivam, A. Murthy, E. Belding-Royer. Dynamically adaptive multipath routing based on AODV. In Proc. 3rd Annual Mediterranean Ad Hoc Networking Workshop, 2004..

[19] S. Bouam and J. Ben-Othman, "Data Security in Ad Hoc Networks Using Multipath Routing," Proc. PIMRC 2003, vol. 2, pp. 1331–1335, Sept. 2003.

[20] S.-J. Lee and M. Gerla. Split multipath routing with maximally disjoint paths in ad hoc networks. In IEEE Proceedings of ICC 2001, pages 3201–3205.

[21] W. Lou and Y. Fang, "A Multipath Routing Approach for Secure Data Delivery," Proc. MILCOM 2001, vol. 2, pp. 1467–1473, Oct. 2001.

[22] Y. Yuan, H. Chen, M. Jia. An optimized ad-hoc on-demand multipath distance vector (AOMDV) routing protocol. In Communications, IEEE Asia-Pacific Conference, 2005 (pp. 569-573).

[23] Z. Li, Y. Kwok. A new multipath routing approach to enhancing TCP security in ad hoc wireless networks. In IEEE Parallel Processing, 2005. ICPP 2005 Workshops. International Conference Workshops, 2005, (pp. 372-379).

Authors' Profiles

KHAN Koffka, was born in San Fernando, Trinidad and Tobago in 1978. He received the B.Sc. and M.Sc. degrees from University of the West Indies, in 2002 and 2008, respectively. He was awarded by the University of the West Indies for his contributions made in postgraduate work in 2009 as a research assistant. He is presently a student at The University of The West Indies; St. Augustine Campus (TRINIDAD & TOBAGO) in the Department of Computing and Information Technology (Faculty of Science & Agriculture). He has up-to-date, published twelve papers in journals of international repute & in fourteen proceedings of international conferences.

GOODRIDGE Wayne, is a Lecturer in the Department of Computing and Information Technology, The University of the West Indies, St. Augustine. He did his PhD at Dalhousie University and his research interest includes computer communications and security.

How to cite this paper: Koffka Khan, Wayne Goodridge,"Impact of Multipath Routing on WSN Security Attacks", International Journal of Intelligent Systems and Applications(IJISA), vol.6, no.6, pp.72-78, 2014. DOI: 10.5815/ijisa.2014.06.08