Life Expectancy Analysis of DSR and DSDV Protocol in MANET with Dos Attack

Muhammad Izwan Idris[1], Abdul Hadi Abd Rahman[1],*, Pei-Chun Lin[2] and Patrick C. K. Hung[3]

[1]Center for Artificial Intelligence Technology, Universiti Kebangsaan Malaysia
[2]Department of Information Engineering and Computer Science, Feng Chia University
[3]Faculty of Business and Information Technology, University of Ontario Institute of Technology
Corresponding author email: abdulhadi@ukm.edu.my

Summary
Mobile ad hoc Network (MANET) is an infrastructure-less multi-hop wireless network. A node communicates directly with other mobile nodes without any established architecture. To maintain the availability of ad-hoc network, previous works present good routing protocol such as ad hoc on Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Destination Sequenced Distance Vector (DSDV), Reverse ad hoc on Demand Distance Vector (RAODV), ad hoc on demand Multipath Distance Vector (AOMDV), and Temporarily Ordered Routing Algorithm (TORA). However, there are issues and disadvantages of MANET which is the main focus in the existing studies including energy conservation and security threats such as the Denial of Service (DoS) attack. This study was conducted to analyse the energy utilization of reactive protocol, DSR and proactive protocol, DSDV in the situation of a DoS attack. Comparisons are made between the density of malicious nodes ranging from one and three nodes. The purpose of this comparison is to identify the number of malicious nodes that create the worst impact on energy consumption in case of a DoS attack. Network Simulator (NS) version 2.35 is used with the Black Hole code, which is the type of DoS threat that has been selected for the purpose of studying the relative energy consumption and performance varying the routing protocols. Performance of energy and routing protocols was examined based on the energy consumption and network lifetime expectancy metrics. The results of the study showed that DSDV protocol had a greater impact than DSR for single Black Hole attack on the energy consumption and network life. Whereas with the cooperative attack of three malicious nodes, the energy consumption of DSDV protocols was seen to be low due to the shorter life of node in the network as compared to DSR. The results of this study may help in evaluating the impact of Black Hole attack on energy consumption behaviors in the network such as Black Hole attack detection, security protocol improvement and others.

Key words:
MANET, energy consumption, dsdv, dsr

1. Introduction

From the revolutionary developments in wireless technology have to some extent promoted the use MANET. The striking increase in sensor applications during the past two decades indicates a revolution such as caused by the development of a microcomputer in 1980's is in the offing. The use of sensors in industry and various other fields has grown and these fields have experienced transformations in this technology. Nowadays, MANET applications are widely used in industries and fields, such as military, rescue operations, environmental monitoring, health monitoring, habitat monitoring and others.

MANET is an infrastructure-less multi-hop wireless network. Node communicates directly with other mobile nodes without any established architecture. Maintaining the availability of ad-hoc network needs a good routing protocol. Many protocols were developed to address this requirement and they were divided into several classes. DSR and DSDV are among high energy-efficient routing protocols. These protocols are reserved for mobile ad-hoc networks, with the goal of achieving efficient network routing [1].

Denial of Service (DoS) is the most frequent network security attack threatening MANET [2]. Black Hole is classified as one of the DoS attacks according to Salehi et al. [3], which a common means of attacking the mobile ad-hoc network. When Black Hole attacks a network, it affects the performance of the network, especially causing an end-to-end delay and affecting the throughput [4]. In addition to the two performance metrics stated above, there is another performance measurement metrics to be analyzed to evaluate the impact of the attack to MANET network.

Recognizing the needs for research in the performance of MANET, this study was undertaken with that objective. This paper compares and attempts to understand the correlation of performance for the given MANET routing protocol, DSDV and DSR when not under attack and under a single and collaborative DoS attack. Network Simulator (NS) version 2.35 is used to study the performance based on the total energy consumed and network lifetime.

This paper is organized as follows: Section 1 discusses the background of this study. In section 2 major issues in MANET, high energy efficient routing protocols, specifically DSDV & DSR and types of attack in MANET are described. Section 3 elucidates the methodology used in this study and section 4 presents the findings and discussion. Lastly in section 5 concludes the paper with a summary of the findings and recommends future works.

Manuscript received March 5, 2020
Manuscript revised March 20, 2020

2. Related Works

The two main issues in the wireless sensor network and MANET were energy conservation and network security [5,6,7]. Preserving energy is important because the nodes are supplied out of a limited battery capacity. Therefore, energy consumptions of these nodes needs to be carefully controlled. For this purpose, the operation of each node, its energy needs and the source of energy need to be analyzed to maintain the effectiveness of the network. There are many security issues primarily with MANET because the security aspect was not addressed. As such, many flaws in the existing protocols make them vulnerable to various types of attacks in various fields in which they are used.

2.1 Overview of MANET Routing Protocols

High energy-efficient routing protocols is crucial in MANET operations. Portable nodes utilize batteries and have limited energy supply. Also, their networks are subject to dynamic changes in topology environments. Hence the use of energy-efficient protocols will increase the lifespan of the nodes through energy saving [8]. There are various routing protocols in MANET as shown in Fig. 1. These protocols are classified into three categories: Proactive, Reactive and Hybrid routing protocols [9]. The protocols are built with the aim of handling a large number of nodes with restricted energy resource. Main concern in routing protocol is mobility of the nodes at various location. The key is to reduce the routing-message overhead as the number of mobile nodes increases.

2.1.1 Destination Sequence Distance Vector (DSDV)

DSDV protocol maintains a routing table to all destinations, the number of nodes to reach the destination and sequence number set by the destination node [9]. Sequence number is used to distinguish expired routes from the new one and thus avoid the formation of routing loops. Therefore, this update is driven by time and by events. Routing updates can be sent in two ways, namely full updates or incremental updates. The full update involves sending the full routing tables to the adjacent nodes and it can be sent in multiple packages. The incremental updates involve sending only routes that have metric changes since last update.

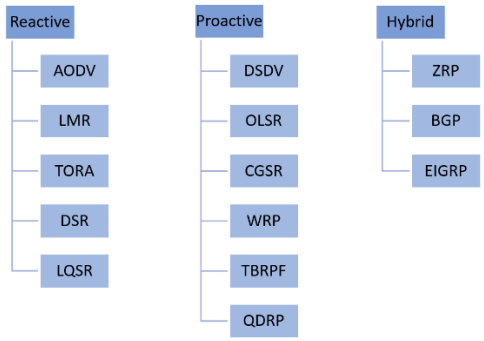

Fig. 1 Types of Routing Protocols in MANET (Lalar & Yadav 2017)

2.1.2 Dynamic Source Routing (DSR)

DSR is reactive, on-demand routing protocol based on the source routing. It is among of the well-known protocols in the category [10]. Based on the study, it is observed that since DSR and AODV protocols have a similar performance, both protocols are often used as research material related to reactive routing protocol in MANET [11]. DSR is a source-based, which means the route is made only when required by the source node. When a source node sends a packet to an unknown destination, it starts the route discovery process to find the destination node. Route request package (RREQ) is sent to the node next to the source. This RREQ contains source node address, destination node address, and unique identification number (ID). The receiving node adds its own address to the RREQ route record and forwards it to the next node. If that is not the destination and has no route to the destination.

2.2 Type of Attacks in MANET

Due to limitation found in mobile ad-hoc networks, research in designing security mechanism that meet the various aspects and characteristics of MANET becomes difficult. Among the limitations are inadequate energy supply, limited storage capacity, unreliable communication and high communication latency [12,13]. This makes MANET vulnerable to threats and security attacks. There are two main purposes of attack against network and routing protocols. First is to intercept confidential information such as data from military and security networks. Second is for network services interruption through the energy reduction of all nodes in the network [14]. According to Panda and Pattanayak [8], Black-hole and Worm-hole were the most frequently used means of executing denial of service attacks on MANET [15, 16].

2.2.1 DoS Attack

DoS attack causes a network to be disrupted or paralyzed. As a result, network capability is reduced and it fails to perform its specific functions [2, 17]. Black Hole is a type

of DoS attack and it occurs when a malicious node intentionally intercepts and damages the data. Malicious node also attacks the routing control messages. Attacker sends a Route Reply (RREP) on the Route Request (RREQ) message and claims that it has a shorter route to the destination. Message is sent before the source node gets the answer from its neighbor node. Therefore, the malicious node misleads its source and sets the route through itself. With the assumption that the routing update from malicious node is correct, data from all other nodes gets sent through malicious node, which creates a Black Hole in the network in which all the data goes. Malicious node captures all packets data and discards them. Figure 2 depict a mobile ad-hoc network with Black Hole attack.

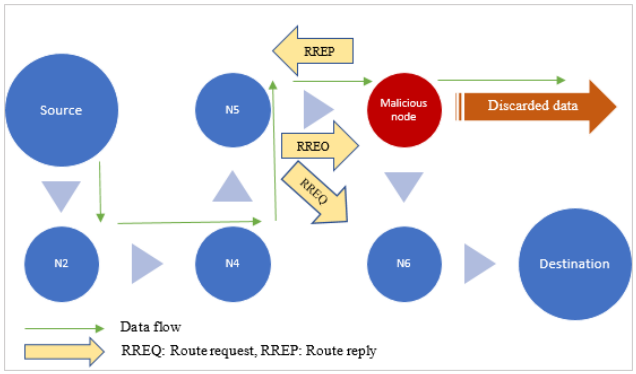

Fig. 2 Mobile ad-hoc network with Black Hole attack

3. Simulation Environment

3.1 Black Hole setting

To study and compare the energy consumption and performance of the above-mentioned protocols, various application can be used to perform network simulation such as QUALNET, NS-2, OPNET, MATLAB and OMNET. Among the applications that support DSR and DSDV protocols are Network Simulator 2 (NS-2.35), which was selected for this study. While simulating networks for Black Hole attack, some configuration files of the application were modified. The simulation parameters are listed in Table 1.

The codes for Black Hole attacks are not provided in NS-2.35. To create an attack in MANET, additional code was required and modifications to some DSR and DSDV protocol files were made. Figure 3 presents the added algorithm for the malicious node generated sending fake route reply. Furthermore, a code for dropping packet is created to handle the malicious node as shown on Fig. 4.

Table 1: Simulation parameter

Parameter	Value
Simulator	Ns-2 (ver 2.35)
Simulation time	360 s
Number of nodes	20
Number of malicious nodes	1, 3
Routing protocol	DSDV, DSR
Traffic model	TCP/FTP
Node speed	5 m/s – 10 m/s
Network area	100m x 50m
Waypoint	RWP
Energy Model	energyModel
Initial Energy	2J

```
//Added for Blackhole Attack
//Malicious node generates fake route replies using following code

else if(malicious==true)
{
Entry *e == max(Entry *e, prq->prq.dst_Entry *e)+1;
 if (Entry%2) Entry++;

Packet::free(p.pkt);
}
#endif
```

Fig. 3 Code sending fake route reply in file dsragent.cc

```
void
DSRAgent::handleForwarding(SRPacket &p)
  /* forward packet on to next host in source route,
   snooping as appropriate */
{
  hdr_sr *srh =  hdr_sr::access(p.pkt);
  hdr_ip *iph = hdr_ip::access(p.pkt);
  hdr_cmn *ch =  hdr_cmn::access(p.pkt);
  bool flowOnly = !srh->num_addrs();

// Added for Blackhole Attack
// If the node is a malicious node - drop the packet
        if (malicious == true ) {
           drop(p.pkt, DROP_RTR_ROUTE_LOOP);
           return;
        }
```

Fig. 4 Code for dropping packet in file dsragent.cc

3.2 Performance Metrics

Few network performance metrics were used through the simulation experiments for the MANET protocols defined below:

3.2.1 Total Energy Consumed

Total energy consumption [18] of all node during the simulation can be calculated through:

TotEnergyConsumed = (IniEnergy * NumNodes) – remEnergy (1)

3.2.2 Network life expectancy

Measured by the first node exhausted in the circuit [19].

4. Results and Discussion

4.1 Analysis of network lifetime

In DSDV protocol, based on the graph in Fig. 5, in all three scenarios, the life span of the network was observed to expire before the simulation time ended. The utilization of energy is influenced by various factors such as DSDV protocol properties, node numbers and non-stop node movements until the simulation is over. Each node movement will cause the routing table to send an update. In simulation without attack, the life span is 250 seconds, while with a 1-node attack, the lifetime is reduced to 194 seconds and with a 3-node attack the life span is shortened to 20 seconds.

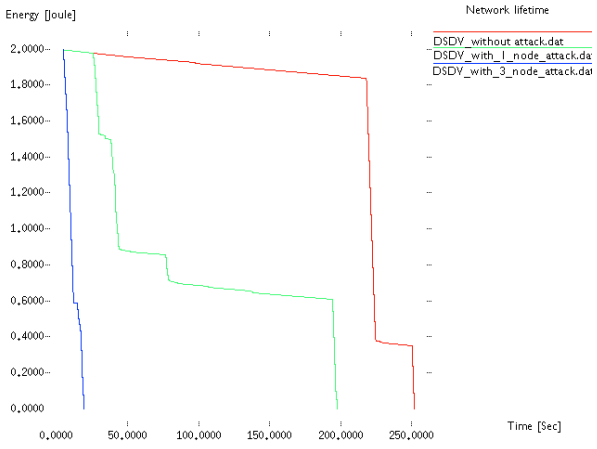

Fig. 5 Graph of network lifetime for DSDV

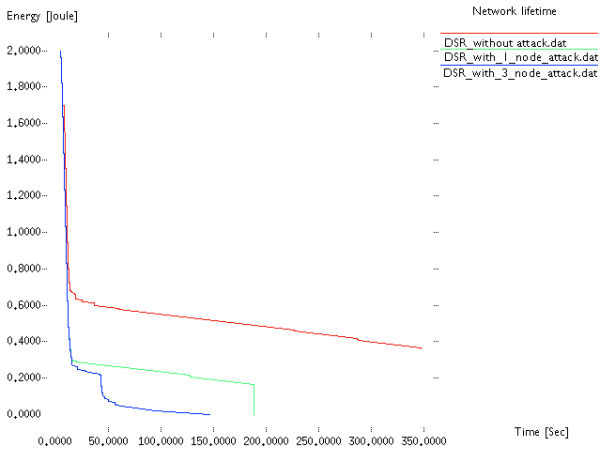

Fig. 6 Graph of network lifetime for DSR

For DSR protocol, results are quite different as shown in Fig. 6. Without attack, the life span of the network shows that energy is available throughout the simulation period. However, in the presence of 1 malicious node, the network life span drops and expires in 188 seconds. In case of a 3-node attack, life span ends in 146 seconds. Reduction of lifetime is fairly consistent and influenced by various factors.

4.1 Analysis of total energy consumption

The network energy consumption for both protocols can be seen in Fig. 7. For DSDV protocol, energy consumption increased tremendously in the presence of 1 malicious node. It was 18.32 Joules compared to 13.37 Joules when not under attack. While in a 3 malicious nodes attack, network energy consumption decreased to 13.65 Joules. As previously mentioned, the lifespan of DSDV network under a 3 malicious nodes attack expires in as early as 20 seconds. This is the factor for reduced energy consumption. FTP transactions cannot be performed due to lack of energy so no packet data is forwarded by other nodes. In contrast with DSR analysis results, energy consumption is consistently increasing in small quantities. The scenario without attack shows the energy consumption of 14.22 Joules followed by energy consumption at 14.93 Joules under 1 malicious node attack. For 3 malicious nodes attack, the energy consumption was 15.88 Joules.

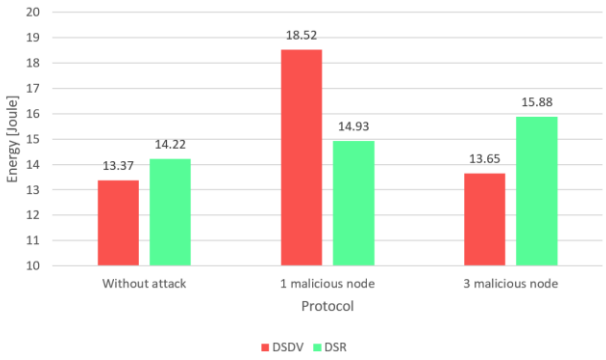

Fig. 7 Graph of total energy consumption

4.2 Analysis of network life expectancy and total energy consumption

Table 2 presents the performance result of DSDV and DSR for network life expectancy and energy consumption in three different scenarios. The impact on MANET's network life span during Black Hole attacks depends on the number of malicious nodes in the network, and the type of protocol used. DSDV protocol, with 1 malicious node attack, the lifetime reduction compared to without attack score at a value of 22.4% while with the attack of 3 malicious nodes, the lifetime reduction is 92% as compare to lifetime without attack. Significant decrease of 89.67%in network lifetime is seen when the number of malicious nodes increased from 1 to 3 nodes. Looking at DSR protocol, with 1 malicious node the lifetime reduction rate is higher than in the previous protocol, which was at 47.77%. This indicates the nature of the protocol in the presence of malicious nodes. However, with the attack of 3 malicious nodes, the difference recorded was at 59.44% and no significant decrease in lifetime was observed between 1 and 3 malicious nodes attack, which

was 22.34%. The lifetime declination for DSR protocols is seen to be more consistent.

Table 2: Value and Percentage difference of Performance Metrics

Scenario	Metric	Value		% Different
		DSDV	DSR	
Without attack	Life expectancy	250 secs	360 secs	36.06 %
	Total energy	13.37 Joule	14.22 Joule	6.16 %
1 malicious node attack	Life expectancy (compare no attack)	194 secs (-22.40%)	188 secs (-47.77%)	3.14 %
	Total energy	18.52 Joule	14.93 Joule	21.46 %
3 malicious node attack	Life expectancy (compare no attack)	20 secs (-92.00%)	146 secs (-59.44%)	151.80 %
	Total energy	13.65 Joule	15.88 Joule	15.10 %

4.3 Effect of Black Hole attack to energy consumption

Both protocols showed energy consumption without a Black Hole attack differing by a small margin, DSDV uses 13.37 Joules, while DSR uses 14.22 Joules. With 1 malicious node attack, energy consumption for DSDV protocol increased to 18.52 Joules (an increase of 5.15 Joule). While under attack from 3 malicious nodes, the energy consumption dropped significantly to 13.65 Joules. The earlier analysis found that network lifetime for DSDV Under attack from 3 malicious nodes is only 20 seconds, so the energy uses for the node performing FTP transactions stopped at this time and no packet data was forwarded by other nodes. This caused less energy consumption. For DSR protocols, there is a marginal increase in energy consumption in the presence of attacks. The attack by 1 malicious node showed an increase of 0.68 Joule while with the attack of 3 malicious nodes, the increase was 1.66 Joules.

4.4 Summary

Studies have shown that Black Hole attacks affect the performance of MANET. The performance metrics used for the study are the network lifetime and total energy consumption and they are showing the impact from the attack. The following is the summary of the analysis conducted in this study.

- The average network lifetime decreased during the Black Hole attack on both DSR and DSDV protocols. The number of malicious nodes affects the lifetime value.
- The network lifetime of DSDV protocol showed a significant decrease of 92.00% with a 3 malicious node attack. While for the DSR protocol, the decrease was only 59.44%.
- The amount of energy consumed by the network increases with a 1 malicious node attack. DSDV protocol showed a substantial increase of 38.31%. While for DSR protocol, only 4.99% increase is recorded.
- The amount of energy used by the network under a 3 malicious node attack shows the difference between the two protocols. DSDV indicates a decrease in energy consumption. This is due to energy on node performing FTP transmission control depleted as early as 20 seconds because of no data traffic is forwarded to other nodes in the network thus energy consumption is lesser than in case of 1 malicious node attack. While for DSR protocols, energy consumption is increased by 11.67%.
- Maximum impact on Black Hole attack can be seen on DSDV protocols due to a very short network lifetime with the attack of 3 malicious nodes and a high amount of energy consumption recorded with just 1 malicious node attack.

5. Conclusion

DoS attacks in MANET is difficult to discover. Further studies on network behavior when under attacks occur are required and complete set of data for each MANET scenario needs to be recorded. This is to ensure that any anomalies or unusual activities within the network can be tracked instantly. Recommendation of scope for the future works can be based on the initial position of the nodes, the distance between the nodes, whether nodes are static of show random mobility, use of different energy models, using different initial energy values for regular and malicious nodes and the size of topographies other than those implemented in the previous studies.

Acknowledgments

The authors want to thank the University Kebangsaan Malaysia for supporting and funding this research, grant code: GGPM-2017-040.

References

[1] Royer, E.M. & Toh, C.K. 1999. A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. IEEE 1070-9916/99.

[2] Patil, S. & Chaudhari, S. 2016. DoS attack prevention technique in Wireless Sensor Networks. Procedia Computer Science 79 (2016) 715 – 721.

[3] Salehi, M. & Samavati, H. 2012. Evaluation of DSR Protocol under a New Black hole Attack. IEEE 978-1-4673-1148-9/12.

[4] Wazid, M., Katal, A. Singh, R. S. Goudar, R. H. & Singh D. P. 2013. Detection and prevention mechanism for black hole attack in Wireless Sensor Network. IEEE 978-1-4673-4866-9/13.

[5] Du, J. & Li, J. 2011. A study of security routing protocol for Wireless Sensor Network. IEEE DOI 10.1109/IMCCC.2011.68: 236-240.
[6] Xiaomei, Y. & Ke, M. 2016. Evolution of Wireless Sensor Network security. IEEE.
[7] Tian, L., Du, H. & Huang, Y. 2012. The simulation and analysis of LEACH protocol for wireless sensor network based on NS2. IEEE 978-1-4673-0945-5/12.
[8] Panda, N. & Pattanayak, B.K. 2018. Analysis of Blackhole Attack in AODV and DSR. DOI: 10.11591/IJECE.V8I5: 3093-3102.
[9] Daas, A., Mofleh, K., Jabr, E. & Hamad, S. 2015. Comparison between AODV and DSDV Routing protocols in Mobile Ad-hoc Network (MANET). IEEE 978-1-4799-7626-3/15.
[10] Kumar, D., Srivastava, A., Gupta, S.C. 2012. Performance Comparison of Pro-active and Reactive Routing Protocols for MANET. DOI: 10.1109/ICCCA.2012.6179226
[11] Hu, B. & Gharavi, H. 2007. DSR-Based Directional Routing Protocol for Ad Hoc Networks. IEEE 978-1-4244-1042-2. DOI: 10.1109/GLOCOM.2007.936.
[12] Lalar, S. & Yadav A.K. 2017. Comparative Study of Routing Protocols in MANET. DOI: 10.13005/OJCST.V10(1):174-179.
[13] F.A Jalin, N. E Othman, R. Hassan, A.H.A Rahman, D.P.D Sikumbang, K.A.A Bakar. 2018 An Implementation Study of DMM PMIPV6 Protocol on Dual-Stack Network Environment. Asia-Pacific Journal of Information Technology and Multimedia. 7(1). 29-44.
[14] Majumdar, A. & Sarkar, D. 2015. Various types of routing protocols in Wireless Sensor Network with vulnerabilities: a review. IEEE 978-1-4799-6908-1/15: 1-7.
[15] Bansal, V. & Saluja, K. K. 2016. Anomaly based detection of black hole attack on leach protocol in WSN. IEEE 978-1-4673-9338-6/16.
[16] Ahmed Khan, Z. & Islam, M.H. 2012. Wormhole Attack: A new detection technique. IEEE 978-1-4673-4451-7/12.
[17] Hari, P. B. & Singh, S. N. 2016. Security issues in Wireless Sensor Networks: current research and challenges. IEEE 978-1-5090-0673-1/16.
[18] Gouda, B.S., Mandal, A.B., Narayana, K.L. 2012. Simulation and Comparative Analysis of Energy Conservation Performance Metric for ERAODV, AODV and DSDV Routing Protocols in MANET. IEEE 978-1-4673-4805-8/12.
[19] Priyadharshini, C. & ThamaraiRubini, K. 2012. PSO Based Route Lifetime Prediction Algorithm for Maximizing Network Lifetime in MANET. IEEE 978-1-4673-1601-9/12.

Corresponding author, Abdul Hadi Abd Rahman received the B.S. and M.S. degrees in Computer Engineering and Computer Science (Network) UTM and UPM in 2006 and 2009, respectively. He was awarded with Doctoral degree from UTM in 2016. He has in internship at Tokai University in during his PhD study. He is now with Center of Artificial Intelligence Technology in UKM.