Research Journal of Applied Sciences, Engineering and Technology 11(3): 299-307, 2015
DOI: 10.19026/rjaset.11.1720
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: January 28, 2015 Accepted: March 1, 2015 Published: September 25, 2015

Research Article

Clustering and the Impact of Grayhole Attack in MANET

M. Ashwin and M. Azath
Department of Computer Science and Engineering, Karpagam University, Coimbatore, India

Abstract: Mobile Adhoc Network (MANET) does not rely on fixed infrastructure as opposed to wireless networks with infrastructure where users communicate directly with an access point or base station. The network is an autonomous, transitory mobile nodes association communicating over wireless links. Nodes in each other's range communicate directly and discover each other dynamically. To ensure intra node communication when not in other's send range, intermediate nodes act as routers relaying packets to destinations. Due to a wireless medium, security in such networks is compromised through many techniques. Grayhole attack is a common attack in MANETs. A simple grayhole attack allows malicious nodes to stop packets in a network and refuse to forward or drop messages passing through. This study investigates the impact of grayhole attack on Quality of Service (QoS) of MANETs. A weighted clustering algorithm is proposed and the impact of maliciousness investigated.

Keywords: Clustering, grayhole attack, Mobile Adhoc Network (MANET), packet forwarding misbehavior

INTRODUCTION

MANETs are collection of wireless mobile nodes that dynamically and temporarily form a network without a central administration and without fixed infrastructure (Murthy and Manoj, 2004). Every MANET node moves arbitrarily making a multi-hop network topology change randomly and unpredictably. A distinctive MANET feature is that a node must act as router to locate optimal path to forward packets. As nodes are mobile, entering and leaving a network, network topology changes continuously. MANETs are an emerging technology for civilian and military applications. MANETs are used in emergency applications due to its self-configuration and easy node deployment. As the communication medium is wireless, only limited bandwidth is available. Another constraint is energy due to node mobility (Manickam *et al*., 2011).

MANET networks are classified as single hop and multi-hop. Nodes in a single hop network in transmission range communicate with others directly. There are a lot of ways to classify MANET routing protocols, based on how protocols handle packet delivery from source to destination. Routing protocols are classified as Proactive, Reactive and Hybrid protocols as in Fig. 1 (Abolhasan *et al*., 2004).

Proactive Protocols are also called table driven protocols where routes to all nodes are maintained in a routing table. Packets are transferred over a predefined route specified in a routing table. Examples are DSDV and Optimized Link State Routing (OLSR).

Reactive Protocols are also called on-demand routing protocols where routes are not predefined. A Source node calls for a route discovery to determine a new route when transmission is needed. Examples are Dynamic Source Routing (DSR) and Adhoc On-demand Distance Vector Routing (AODV).

Hybrid protocols are reactive and proactive protocol combinations. Its benefit is that it has all the pluses of both protocols and so routes are found quickly in a routing zone. Zone Routing Protocol (ZRP) is an example.

Cluster-based routing in MANETs solves nodes heterogeneity and limits routing information inside a network. The idea behind clustering is to group network nodes in many over lapping clusters. Clustering ensure hierarchical routing where paths are recorded between clusters instead of between nodes increasing routes life and lowering routing control overhead. Inside a cluster, a node that coordinates cluster activities is called Cluster Head (CH). There are ordinary nodes also inside a cluster with direct access to this cluster head and gateways. Gateways are nodes that hear two or more CHs. Ordinary nodes send packets to their CH that distributes packets inside a cluster, or (if destination is outside a cluster) forwards them to a gateway node for delivery to other clusters. By replacing nodes with clusters, current routing protocols can be directly applied to networks. Only gateways and CHs participate in routing control and update messages propagation (Agarwal and Motwani, 2009).

MANET security is challenging due to lack of centralized infrastructure and management, open

Corresponding Author: M. Ashwin, Department of Computer Science and Engineering, Karpagam University, Coimbatore, India

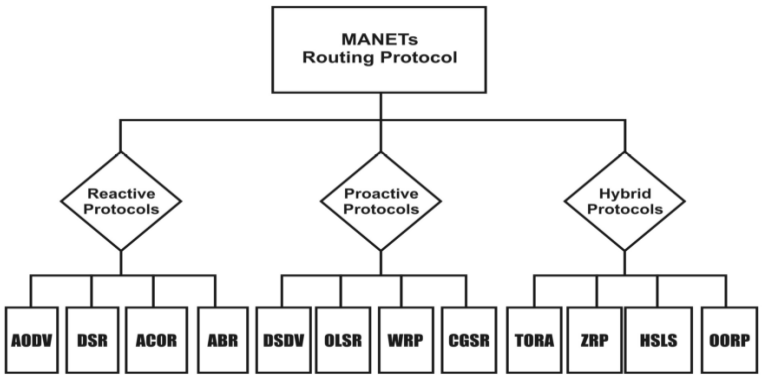

Fig. 1: MANET routing protocols

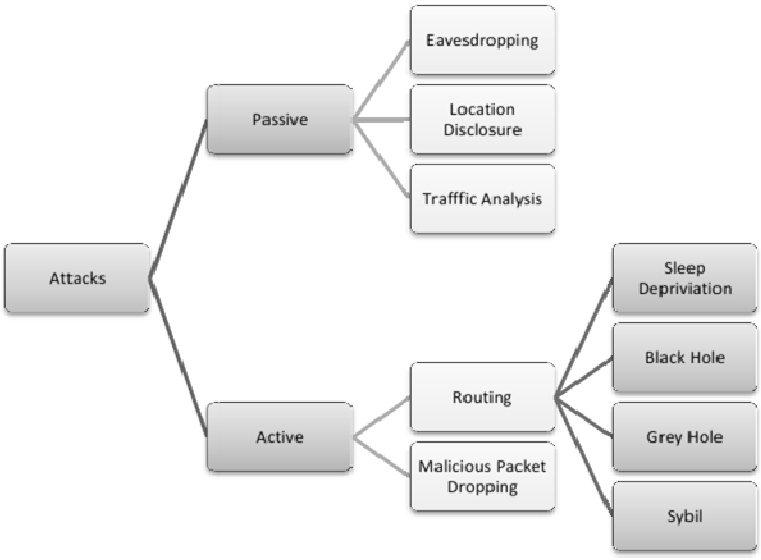

Fig. 2: Classification of attacks in the network layer in MANET

environment, random node distribution in space and changing topology, thereby making MANETs vulnerable to attack (Peethambaran and Jaayasudha 2014). Some issues are:

- There are no central points for data collection
- MANET routing protocols rely on intermediate nodes, which enable attackers to intrude
- As MANETs are mobile, there is no fixed topology, so intrusion detection is complicated
- Mobile nodes often have limited power, limited computing abilities and memory making ID process complex

Here nodes are not protected much physically. So attackers easily attack nodes and they are used to launch many kinds of attacks. Routing protocols assume that all network nodes are well behaved and are not malicious. So attackers also insert malicious nodes into a network. An Intrusion Detection System (IDS) designed explicitly for MANETs are needed as unlike traditional networks, MANETs lacks a centralized management system. There are many types of intrusions or attacks known on MANETs. Like all attacks, here also the first classification is as passive and active attacks as seen in Fig. 2.

Routing protocols working is not disturbed during passive attacks but instead collects information by analyzing traffic. Information includes network topology, identity, location and details about network nodes. Described below are some passive attacks (Johnson and Maltz, 1996):

Eavesdropping: A big disadvantage of wireless communication, aids such attacks. A communication can be intercepted by another device with a transceiver and located in transmission range. Sometimes encryption prevents attackers from getting information. But when there is no encryption, then attackers get needed information easily.

Traffic analysis and location disclosure: Similar to eavesdropping, nodes locations are identified by a thorough analysis of traffic patterns, frequency and

transmissions between nodes. For example in a situation involving a commanding centre; that centre will receive and send additional communications. So, an attacker easily finds the commanding centre by analyzing the communication/traffic pattern.

Modification of transmitting, injecting, duplicating and packets dropping are some active attacks which cause chaos in MANETs. This is induced by one attacker or as a cooperative effort of more than one attacker called colluding nodes. They disturb network functioning and decrease network performance e.g., denial of service attack. Described below are some active attacks.

Malicious packet dropping: Route discovery establishes a route between a source and destination. To ensure successful packet transmission, a route's intermediate nodes must forward the packets. But malicious nodes may decide to drop them. This is also called data packet dropping attack or data forwarding misbehaviour.

Routing attacks: Malicious nodes utilize loop holes in routing algorithms and the algorithms distributive or cooperative nature to attack. Examples are AODV and DSR.

Four types of routing attacks are discussed:

- **Sleep deprivation attack:** A node interacts with other nodes with the aim of keeping the victim busy.
- **Black hole attack:** When a malicious node is chosen as a route's intermediate node, they may drop packets instead of forwarding them.
- **Grayhole attack:** Similar to black hole attack, the difference being that here packets is dropped selectively.
- **Sybil attack:** An attacker node sends control packets with different identities and creates chaos in a routing process.

This study proposes a weighted clustering algorithm. The new method is evaluated in malicious and non-malicious networks.

LITERATURE REVIEW

Detection of grayhole and taking corrective measures against them was carried out by Sharma and Singh (2013). It also includes comparative analysis of the new technique with earlier work based on number of failures, Average packet delivery ratio, Average network life, Average packet drop Ratio and throughput. Future work can improve the technique's dynamicity and be analyzed in real time scenarios.

A security mechanism to support against a cooperative grayhole attack on MANETs AODV routing protocol was proposed by Sen *et al*. (2007). The new mechanism does not apply cryptographic primitives on routing messages. Simulation showed that the scheme had a significantly high detection rate with moderate network traffic overheads.

A new solution against grayhole attack was proposed by Wei *et al*. (2007). The proposal consists of 2 related algorithms: the key management algorithm based on gossip protocol and aggregate signatures based detection algorithm. Simulation with ns2 showed that routing packet overhead was low and packet delivery rate improved.

A technique to detect group grayhole attack through destination based scheme was presented by Kumar and Chawla (2012). This study proposed a method to identify cooperative malicious nodes through a destination based routing method.

A hybrid approach to prevent black and grayhole attacks by selecting second shortest route to secure route selection was presented by Khattak (2013). AODV is a prominent MANET reactive routing protocol. Black and Grayhole attacks are launched on AODV exploiting minimum hop count base route selection strategy.

MR-AODV was proposed by Jhaveri (2013) to detect Blackhole and Grayhole nodes during route discovery. They proposed a modified version to improve MANET performance and also analyzed the new solution evaluating its performance using Network Simulator-2 (NS-2) under varied network parameters.

A scheme that uses a second optimal route for data packet transmission and hash function for black and grayhole attack avoidance and data integrity was proposed by Khattak *et al*. (2013). AODV is a routing protocol used for wireless adhoc networks. Black and grayhole are imminent attacks launched on AODV.

A scheme for AODV protocol proposed by Jhaveri *et al*. (2012) detects and removes malicious node by isolating them, to ensure secure communication. In Grayhole and Black hole attacks, malicious nodes deliberately disrupt network data transmission by sending incorrect routing information.

An algorithm to identify a chain of cooperative malicious node in adhoc networks was proposed by Jain *et al*. (2010). This study proposed a mechanism to detect and remove black and grayhole attacks. This technique is based on sending small sized data of equal size instead of sending it all at once. This algorithm takes O(n) time on average to find a chain of malicious nodes which is better than earlier $O(n^2)$ time bound to detect one black hole network.

The problem of packet forwarding misbehavior was addressed by Banerjee (2008) who proposed a mechanism to detect and remove black and grayhole attacks. This technique can find a chain of cooperating malicious nodes which drop a major portion of packets.

Mechanisms to overcome black hole attack are trust based routing, sequence number comparison, intrusion detection system and Data Routing

Information (DRI) table as proposed by Venkanna and Velusamy (2011). Trust based on demand routing mechanisms identify and decrease hazards by malicious node, in a path. This study ensured a survey of preventing Black hole attacks using trust management mechanism in MANETs.

A Dempster-Shafer (D-S) evidence based trust management strategy was proposed by Yang *et al*. (2014). Simulation was conducted in a Matlab to evaluate the algorithm's performance. Implementation showed good results and proved the advantages of the new method by punishing malicious actions to prevent attack camouflage and deception.

A DSR protocol, aggregate signature algorithm and network model was introduced by Xiaopeng and Wei (2007). This study proposed using aggregate signature algorithm to trace packet dropping nodes. Simulation using ns-2 showed that routing packet overhead was low and that packet delivery rate improved.

An adaptive method to detect black and grayhole attacks in adhoc network based on a cross layer design was demonstrated by Kariya *et al*. (2012). A course-based method to listen into the next hop's action is proposed in a network layer. A collision rate reporting system is formed in MAC layer to guess dynamic detecting threshold and reduce false positive rate under high network overwork. DSR protocol is preferred to test the algorithm.

MATERIALS AND METHODS

It is proposed to investigate grayhole attack impact on MANET QoS. A weighted clustering Algorithm to mitigate malicious nodes impact is proposed.

Grayhole attack: Grayhole attack is an attack on network layer which is an active MANET attack. Grayhole attack is an active attack where an attacking node agrees to forward packets first and then fails to do so, leading to messages dropping. The probability of losing data cannot be predicted in grayhole attacks. In such attacks a malicious node refuses to forward some packets and drops them (Arya and Jain, 2011). Packets from a single IP address or a range of IP addresses are selectively dropped by the attacker who forwards remaining packets. MANET Grayhole nodes are dominant. A node maintains a routing table with the next hop node information. When a source node plans to route a packet to a target node, it uses a specific route, if such a route is possible in its routing table. Or else, nodes start a route discovery process broadcasting Route Request (RREQ) message to neighbours. On receipt of the RREQ message, intermediate nodes update their routing tables for a reverse route to the source node. A Route Reply (RREP) message is sent back to source node when the RREQ query reaches either destination node or any node with a current route to that destination (Kumar and Singh, 2014).
Grayhole attacks have two phases:

Phase 1: A malicious node exploits AODV protocol to advertise itself as having a route to the destination node, with the intention of interrupting packets on the spurious route.

Phase 2: In this phase, the nodes drop interrupted packets with a probability. Grayhole attack detection is difficult. Normally in grayhole attacks, the attacker behaves maliciously till packets are dropped and then attains a normal behavior. Both normal node and attacker are same. Due to this, it is very hard to detect in a network such attacks.

Cluster based routing: The process divides a network into interconnected substructures, called clusters. A cluster has a specific node elected as Cluster Head (CH) based on a precise metric or a combination of metrics like identity, degree, mobility, weight and density. CH is a coordinator within the substructure. A CH is a temporary base station in its cluster and communicates with other CHs (Anupama and Sathyanarayana, 2011; Gupta *et al*., 2012). So a cluster is composed of a CH, gateways and members node.

Cluster head: Coordinator of a cluster.

Gateway: A common node between two or more clusters.

Member node (ordinary nodes): A node neither a CH nor gateway. A node belongs exclusively to a cluster independent of neighbors that might reside in different clusters.

In clustering, a representative of a subdomain (cluster) is 'elected' as a CH and a node which serves as intermediate for inter-cluster communication is a gateway. The remaining members are ordinary nodes. Cluster boundaries are defined by transmission area of its CH. With an underlying cluster structure, non-ordinary nodes are dominant forwarding nodes. Cluster formation has 2 approaches: active clustering and passive clustering (Yi *et al*., 2001).

Nodes cooperate to elect CHs by periodically exchanging information, regardless of data transmission in active clustering. But, passive clustering suspends clustering procedure till data traffic commences (Yi *et al*., 2003). It exploits on-going traffic to spread "cluster-related information" (state of a node in a cluster and its IP address) and collects neighbor information through promiscuous packet receptions (Yi *et al*., 2001).

Passive clustering eliminates the control overhead of active clustering, which implies larger setup latency

that is important for time critical applications; this latency is seen whenever data traffic exchange starts. But, in active clustering schemes, a MANET is flooded by control messages, even when data traffic is not exchanged which consumes valuable bandwidth and battery resources (Gavalas *et al*., 2006).

Proposed weighted clustering algorithm: A network formed by nodes and links is represented by an undirected graph $G = (V, E)$, where V represents a set of nodes v_i and E represents set of links e_i. Note that $V's$ cardinality remains same but cardinality of E changes with links creation or deletion. Clustering can be considered as a graph partitioning problem with added constraints. As underlying graph does not reveal any regular structure, graph partitioning optimally (with minimum partitions) regarding certain parameters becomes an NP-hard problem (Bollobás, 1998). More formally, a vertices set $S \subseteq V(G)$, so that:

$$\bigcup_{v \in S} N[v] = V(G)$$

Here, N [v] is neighborhood of node v, defined as:

$$N[v] = \bigcup_{v' \in V, v' \neq v} \left\{ v' \middle| dist(v, v') < tx_{range} \right\}$$

where, tx_{range} is transmission range of v. CH neighborhood is a set of nodes within its transmission range. The set S is called a dominating set so that every vertex of G belongs to S or has a neighbor in S. The dominating set of a graph is the CHs set. It is possible that a node is physically near to a CH but belongs to another CH. For example, a node might be physically closer to a CH over loaded. It then attaches itself to a CH which is far away due to mobility. Nodes may go out of their CH transmission range thereby changing the neighborhood. But, this does not result in a change of dominant set. It may be that the detached node is unable to attach itself to any nodes in a dominant set implying that the existing dominant set can no longer cover entire graph and so the clustering algorithm is invoked to find a new dominant set.

Choosing an optimal number of CHs which yield high throughput but incur low latency, is still an important problem. As search for better heuristics for this problem continues, a new algorithm based on the use of a combined weight metric, that considers many system parameters like ideal node degree, transmission power, mobility and nodes battery power is proposed. Depending on specific applications, any or all parameters are used in metric to elect CHs. A fully distributed system where all nodes in a mobile network share similar responsibility and act as CHs is possible. But, more CHs lead to extra hops for a packet when it is routed from source to destination, as a packet has to traverse many CHs. So, this solution leads to high latency, more information processing and more power consumption per node.

To maximize resource use, choose minimum number of CHs to cover an entire geographical area on which nodes are distributed. The area can be split up into zones, the size of which is determined by nodes transmission ranges. This puts a lower bound on CHs required. To reach this lower bound, uniform node distribution is necessary over same area. Also, total nodes per unit area must be restricted so that a zone's CH can handle all nodes. But, zone based clustering is not viable due to the following reasons. CHs would be centrally located in a zone and if they move, new CHs should be chosen. It might so happen that no other node in that zone is centrally located. Finding a new node which acts as a CH with other nodes in transmission range is difficult. Another problem is due to non-uniform distribution of nodes over an entire area. When a specific zone is densely populated due to migration of nodes from other zones, then CH may not be able to handle all traffic generated by nodes as there is an inherent limitation on node numbers a CH handles. To elect minimum CHs which support all nodes in a system satisfying the above constraints is proposed.

To decide whether a node is suited to be a CH, its degree, transmission power, mobility and battery power are considered. The following features are considered in a clustering algorithm:

- CH election is not periodic and is invoked rarely. This reduces system updates and computation and communication costs. A clustering algorithm is not invoked if relative distances between nodes and CHs are same.
- CH election procedures are not periodic and are invoked rarely reducing system updates and so computation and communication costs are high. A clustering algorithm is not invoked if relative distances between nodes and CHs are unchanged.
- Battery power can be efficiently used in some transmission ranges, i.e., it takes less power for a node to communicate with others when they are close to each other. A CH consumes more battery power than a node as a CH has extra responsibilities for its members.
- Mobility is important in deciding CHs. To avoid frequent CH changes, a CH that does not move quickly should be elected. When CH moves fast, nodes may be detached from it and so re-affiliation occurs. Re-affiliation happens when an ordinary node moves out of a cluster and joins another cluster. In such cases, information exchange between a node and the corresponding cluster head is local and small. Information update during a change in a dominant set is much more than re-affiliation.

- A CH communicates better with neighbors closer to it in transmission range (Wu *et al*., 1997). As nodes move away from a CH, communication may be difficult due mainly to increasing distance.

An algorithm called Weighted Clustering Algorithm (WCA) that combines all the above system parameters with some weighing factors is chosen according to system needs. Power control is important in CDMA networks and so the weight of the corresponding parameter is larger. Flexibility of changing weight factors helps apply the algorithm to various networks. CH election procedure output is a set of nodes called dominant set. According to the notation, nodes that a CH handles are ideally around δ. This ensures that CHs are not overloaded and system efficiency is maintained at expected levels. A CH election procedure is invoked during system activation and when a current dominant set cannot recover all nodes. Each election algorithm invocation does not mean that all CHs in a previous dominant set are replaced by new ones. When a node detaches itself from a current CH and attaches itself to another then both CHs update member list instead of invoking the election algorithm. A basic version of this algorithm appeared in (Chatterjee *et al*., 2000).

Cluster head election procedure: The procedure has eight steps as described below:

Step 1: Find neighbors of every node v (nodes within transmission range) which defines its degree, d_v, as:

$$d_v = \left|N(v)\right| = \sum_{v' \in V, v' \neq v} \left\{dist(v, v') < tx_{range}\right\}$$

Step 2: Compute degree-difference, $\Delta v = \left|d_v - \delta\right|$, for every node v.

Step 3: For every node, compute a sum of distances, D_v, with all neighbors, as:

$$D_v = \sum_{v' \in N(v)} \left\{dist(v, v')\right\}$$

Step 4: Compute running average of speed for every node till current time T. This gives a measure of mobility and is denoted by M_v, as:

$$M_v = \frac{1}{T}\sum_{t=1}^{T}\sqrt{\left(X_t - X_{t-1}\right)^2 + \left(Y_t - Y_{t-1}\right)^2}$$

where, (X_t, Y_t) and (X_{t-1}, Y_{t-1}) are coordinates of node v at time t and (t - 1), respectively.

Step 5: Compute cumulative time, P_v, during which a node v acts as a CH. P_v implies how much battery power was consumed and is assumed more for a CH than an ordinary node.

Step 6: Calculate combined weight W_v for every node v, where.

$$W_v = w_1\Delta_v + w_2 D_v + w_3 M_v + w_4 P_v$$

where, w_1, w_2, w_3 and w_4 are weighing factors for corresponding system parameters.

Step 7: Choose a node with smallest W_v as cluster-head. All neighbors of chosen CH are not allowed to participate in the election procedure.

Step 8: Repeat steps 2-7 for remaining nodes not yet selected as CH or assigned to a cluster.

The first component, $w_1\Delta_v$, contributing to a combined metric W_v helps efficient MAC functioning as it is always desirable for a CH to handle up to a some nodes in its cluster. The motivation of D_v is related to energy consumption. It is known that additional power is required to communicate to a larger distance. Hence, one might think that it would be appropriate to use a sum of squares (or higher exponent) of distances, as power needed to support a link increases faster than linearly with distance (in the far-field region). Attenuation in signal strength is inversely proportional to an exponent of distance, which is approximated to 4 in cellular networks where distance between mobiles and base stations is of an order of 2-3 miles. But in adhoc networks, distances involved are small (approximately hundreds of meters). In this range attenuation is assumed to be linear. The third component for W_v is due to node mobility. A node with less mobility is a better choice for CH. The last component P_v, is measured as total (cumulative) time a node acts as CH. Assuming that battery power of nodes to be same as at the beginning. Then, battery drainage gives a direct measure of available battery power. Also, battery drainage will be more for nodes acting as CHs is considered. But, if nodes have battery power to start with, then it would be accurate metric to measure power available with a node. This depends on a node's initial power and power expended based on network traffic and link length used to support it.

RESULTS AND DISCUSSION

The simulations are conducted for varying number of nodes (40 to 200). The simulations are conducted for without malicious nodes, 10% malicious node and 20% malicious node in the network. The Average packet delivery ratio, Average end to end delay and number of clusters formed are evaluated (Table 1).

Table 1: Average packet delivery ratio

Number of nodes	20% Malicious nodes	10% Malicious nodes	Without malicious node
40	0.677	0.7765	0.9132
80	0.6418	0.7511	0.8559
120	0.6151	0.7341	0.8328
160	0.614	0.7004	0.8243
200	0.5561	0.6681	0.7476

Table 2: Average end to end delay in second

Number of nodes	20% Malicious nodes	10% Malicious nodes	Without malicious node
40	0.002417	0.001991	0.001612
80	0.002948	0.002483	0.001883
120	0.006536	0.002781	0.002411
160	0.009749	0.002889	0.002387
200	0.029765	0.017541	0.014416

Table 3: Number of cluster formed

Number of nodes	20% Malicious nodes	10% Malicious nodes	Without malicious node
40	7	6	6
80	11	9	9
120	14	12	11
160	20	17	16
200	26	21	21

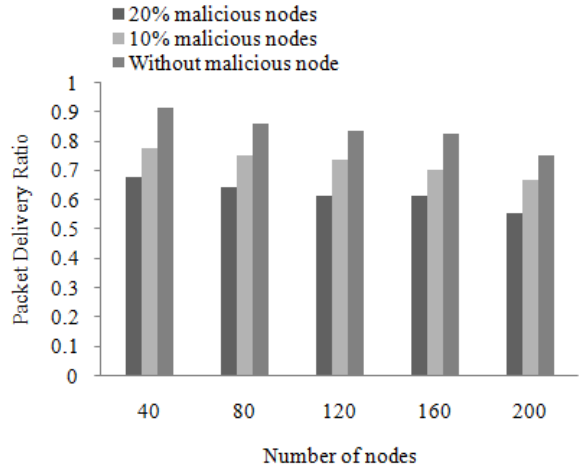

Fig. 3: Average packet delivery ratio

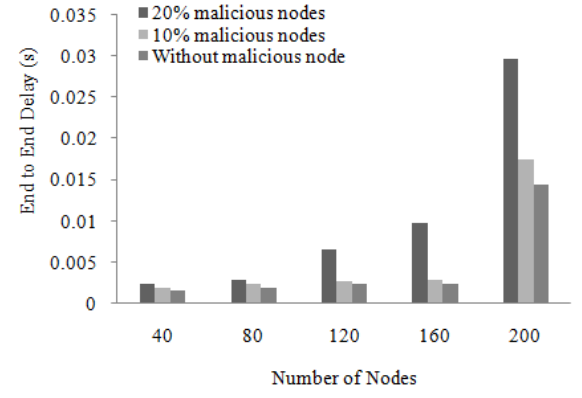

Fig. 4: Average end to end delay in second

As seen from Fig. 3, the packet delivery ratio decreases significantly as the maliciousness increases. When there are no malicious nodes in the network, the packet delivery ratio improves by 16.18 and 21.71% than 10 and 20%, respectively malicious nodes in the network for 40 nodes. When there are no malicious nodes in the network, the packet delivery ratio improves by 11.23 and 29.38% than 10 and 20%, respectively malicious nodes in the network for 200 nodes (Table 2).

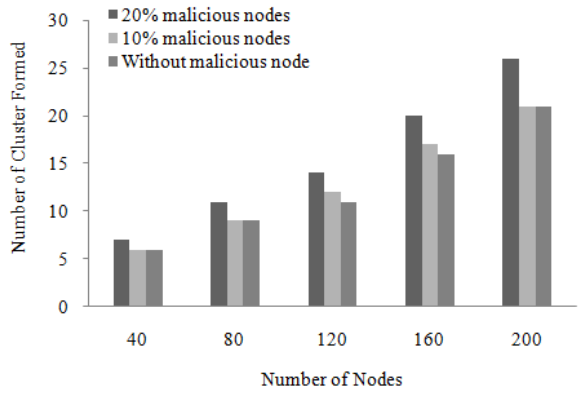

Fig. 5: Number of cluster formed

As observed from Fig. 4, the Average End to End Delay increases significantly as the maliciousness increased. When there are no malicious nodes in the network, the End to End Delay decreases by 21.03 and 39.96% than 10 and 20%, respectively malicious nodes in the network for 40 nodes. When there are no malicious nodes in the network, the Average End to End Delay decreases by 19.56 and 69.48% than 10 and20%, respectively malicious nodes in the network for 200 nodes (Table 3).

As seen from Fig. 5, the number of cluster formed remains same between without malicious nodes and 10% malicious nodes. When there are no malicious nodes in the network, the number of cluster formed is

decreased by 15.38 than 20%, respectively malicious nodes in the network for 40 nodes. When there are no malicious nodes in the network, the number of cluster formed is decreased by 21.28 than 20%, respectively malicious nodes in the network for 200 nodes.

CONCLUSION

This study investigated impact of grayhole attack on MANET QoS. A weighted clustering algorithm is proposed and maliciousness impact was investigated. The new method aimed to choose an optimal number of CHs which yield high throughput but have low latency. CHs are elected based on degree, mobility, transmission and battery power. Simulations evaluated the impact of maliciousness on the network. When there are no malicious network nodes, average packet delivery ratio is high and average end to end delay is low.

REFERENCES

Abolhasan, M., T. Wysocki and E. Dutkiewicz, 2004. A review of routing protocols for mobile ad hoc networks. Ad hoc Netw., 2(1): 1-22.

Agarwal, R. and D. Motwani, 2009. Survey of clustering algorithms for MANET. arXiv preprint arXiv:0912.2303.

Anupama, M. and B. Sathyanarayana, 2011. Survey of cluster based routing protocols in mobile ad hoc networks. Int. J. Comput. Theor. Eng., 3(6): 806-815.

Arya, M. and Y.K. Jain, 2011. Grayhole attack and prevention in mobile adhoc network. Int. J. Comput. Appl., 27(10): 21-26.

Banerjee, S., 2008. Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks. Proceeding of the World Congress on Engineering and Computer Science, pp: 22-24.

Bollobás, B., 1998. Random Graphs. Springer, New York, pp: 215-252.

Chatterjee, M., S.K. Das and D. Turgut, 2000. An on-demand Weighted Clustering Algorithm (WCA) for ad hoc networks. Proceeding of IEEE Global Tele communications Conference (GLOBECOM'00), 3: 1697-1701.

Gavalas, D., G. Pantziou, C. Konstantopoulos and B. Mamalis, 2006. Clustering of mobile ad hoc networks: An adaptive broadcast period approach. Proceeding of the IEEE International Conference on Communications (ICC'06), 9: 4034-4039.

Gupta, N., M. Shrivastava and A. Singh, 2012. Cluster based on demand routing protocol for mobile ad hoc network. Int. J. Eng. Res. Technol. (IJERT), 1(3): 1-4.

Jain, S., M. Jain and H. Kandwal, 2010. Advanced algorithm for detection and prevention of cooperative black and gray hole attacks in mobile ad hoc networks. Int. J. Comput. Appl., 1(7): 172-175.

Jhaveri, R.H., 2013. MR-AODV: A solution to mitigate blackhole and grayhole attacks in AODV based MANETs. Proceeding of 3rd International Conference on Advanced Computing and Communication Technologies (ACCT, 2013), pp: 254-260.

Jhaveri, R.H., S.J. Patel and D.C. Jinwala, 2012. A novel approach for grayhole and blackhole attacks in mobile ad hoc networks. Proceeding of 2nd International Conference on Advanced Computing and Communication Technologies (ACCT, 2012), pp: 556-560.

Johnson, D.B. and D.A. Maltz, 1996. Dynamic Source Routing in Ad Hoc Wireless Networks. Mobile Computing, Springer US, pp: 153-181.

Kariya, D.G., A.B. Kathole and S.R. Heda, 2012. Detecting black and gray hole attacks in mobile ad-hoc network using an adaptive method. Int. J. Emerg. Technol. Adv. Eng., 2(1): 37-41.

Khattak, H., 2013. A hybrid approach for preventing black and gray hole attacks in MANET. Proceeding of 8th International Conference on Digital Information Management (ICDIM), pp: 55-57.

Khattak, H., N. Nizamuddin and F. Khurshid, 2013. Preventing black and gray hole attacks in AODV using optimal path routing and hash. Proceeding of 10th IEEE International Conference on Networking, Sensing and Control (ICNSC, 2013), pp: 645-648.

Kumar, A. and M. Chawla, 2012. Destination based group Gray hole attack detection in MANET through AODV. Int. J. Comput. Sci. Issues, 9(4), ISSN (Online): 1694-0814.

Kumar, K.M. and Y.J. Singh, 2014. A survey on detection and prevention techniques for gray-hole attack in MANET. Int. J. Comput. Sci. Inform. Technol., 5(2).

Manickam, P., T.G. Baskar, M. Girija and D.D. Manimegalai, 2011. Performance comparisons of routing protocols in mobile ad hoc networks. arXiv preprint arXiv:1103.0658.

Murthy, C.S.R. and B.S. Manoj, 2004. Ad Hoc Wireless Networks: Architectures and Protocols. Pearson Education-Prentice Hall, Upper Saddle River, NJ.

Peethambaran, P. and J.S. Jayasudha, 2014. Survey of manet misbehaviour detection approaches. Int. J. Network Secur. Appl. (IJNSA), 6(3).

Sen, J., M.G. Chandra, S.G. Harihara, H. Reddy and P. Balamuralidhar, 2007. A mechanism for detection of gray hole attack in mobile Ad Hoc networks. Proceeding of 6th International Conference on Information, Communications and Signal Processing, pp: 1-5.

Sharma, S. and T. Singh, 2013. An effective intrusion detection system for detection and correction of gray hole attack in MANETs. Int. J. Comput. Appl., 68(12).

Venkanna, U. and R.L. Velusamy, 2011. Black hole attack and their counter measure based on trust management in manet: A survey. Proceeding of 3rd International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom, 2011), pp: 232-236.

Wei, C., L. Xiang, B. Yuebin and G. Xiaopeng, 2007. A new solution for resisting gray hole attack in mobile ad-hoc networks. Proceeding of 2nd International Conference on Communications and Networking in China (CHINACOM'07), pp: 366-370.

Wu, E.H., J. Tsai and M. Gerla, 1997. The effect of radio propagation on multimedia, mobile, multihop networks: Models and countermeasures. Proceeding of IEEE Singapore International Conference on Networks, pp: 411-425.

Xiaopeng, G. and C. Wei, 2007. A novel gray hole attack detection scheme for mobile ad-hoc networks. Proceeding of IFIP International Conference on Network and Parallel Computing Workshops (NPC, 2007), pp: 209-214.

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

Yi, Y., T.J. Kwon and M. Gerla, 2001. Passive Clustering (pc) in ad hoc networks. Internet Draft, draft-ietf-yi-manet-pac-00.txt, November.

Yi, Y., M. Gerla and T. Kwon, 2003. Efficient flooding in ad hoc networks: A comparative performance study. Proceeding of IEEE International Conference on Communications (ICC'03), 2: 1059-1063.