International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 13, Number 7 (2017), pp. 1743-1763

http://www.ripublication.com

DHHP: A Hybrid Technique for Protecting Mobile Adhoc Networks from Selective Packet Drop Attack

Opinder Singh[†], Dr. Jatinder Singh[‡] and Dr. Ravinder Singh[‡]

[†]Research Scholar, IKG PTU, Kapurthala, Punjab, India.
Email: opindermca2008@gmail.com

Abstract

Mobile Adhoc Networks (MANETs) due to their infrastructure less structure are more susceptible to security problems. These networks are unprotected against various types of malicious nodes. Out of the various attacks, selective packet drop attack is the most notorious attack, which reduces the network performance in the terms of various parameters. This type of attack randomly drops the packets in the network and these malicious nodes are very hard to predict. There are various Intrusion Detection Systems (IDSs) proposed so far, in order to prevent the MANETs from selective packet dropping problems. Among the existing mechanisms, Diffie-Hellman and HMAC function based techniques are more suitable countermeasures against selective packet dropping problem in MANETs. There are various shortcomings of these techniques. In this paper, we first describe Diffie-Hellman based and then HMAC (Hash-based Message Authentication Code) based techniques for intrusion detection in MANETs. Then, we have discussed the shortcomings of both of these techniques. In the next section, we proposed a new hybrid technique DHHP (Diffie-Hellman and HMAC based Protection) which utilize the properties of both of these existing techniques for preventing MANETs against selective packet dropping problem. The proposed technique is based on monitoring mode, which removes the limitations of both of the existing techniques and improves the performance of MANETs in the terms of various parameters. The proposed technique is implemented in NS2 simulator and experimental results clearly depict the improved performance of network after isolating the malicious nodes.

Keywords— MANETs, Selective Packet drop attack, Diffie- Hellman, HMAC, DHHP, Intrusion Detection System.

1. INTRODUCTION

A MANET is a wireless network, which consists of various mobile nodes without any fixed infrastructure. In this network, every node acts as a transmitter, data sink, and router. A MANET works in a dynamic environment in which nodes can leave or join the network at any time. Due to dynamic topology and open medium, these networks are more prone to numerous attacks. On these networks, nodes are self-organized in arbitrary fashion. In MANETs, two nodes can directly transfer the data with each other if they are within range. If two nodes are not in the range, then multi-hop routing is used for communication. Due to the dynamic environment in Adhoc networks, wireless link between nodes are highly vulnerable. In these types of networks, bandwidth constrained wireless links are used for communication.

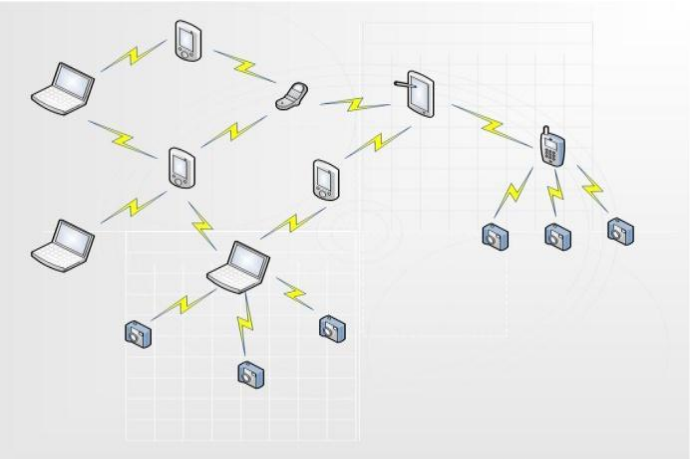

Figure 1. Mobile Ad hoc network

Due to the dynamic topology of MANETs, mobile nodes can move into and out of the range at any time. This movement results in changing routing information of the network. In MANETS, all of the network activities are executed with the nodes themselves. These activities also include the routing activities. Due to Lack of centralized node, dynamic topology, and bandwidth constraint, these networks are highly vulnerable than fixed networks. Because of vulnerabilities, these networks suffer from a number of security attacks. Out of these numerous attacks, it is very hard to detect and prevent from selective packet drop attack.

1.1 Selective Packet Drop Attack

Selective Packet Drop attack is the special case of black hole attack. In this type of attack, malicious nodes selectively drop the packets for deteriorating the efficiency of the network. It is also known as selective forwarding attack. In this attack, malicious nodes change their behavior randomly. Due to this property, these attacks are very hard to detect. In Selective packet drop attack, attacker nodes behave like normal nodes in

most of the time but randomly drop the data packets for reducing the performance of the network. The network under the selective packet dropper attack is shown in figure 2. In this figure, node 14 is the malicious node which is selectively dropping the data packets from source node 0 to destination node 20.

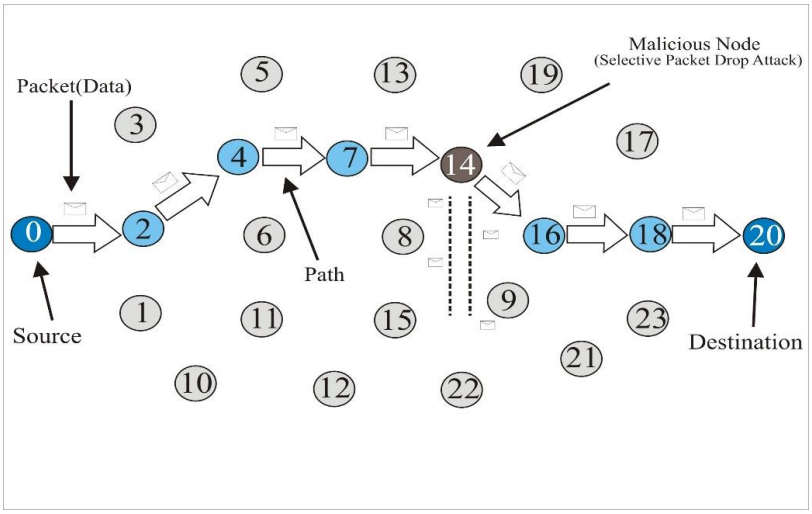

Figure 2. Selective Packet Drop Attack in MANETs

2. RESEARCH OBJECTIVES

The main objective of our study is to discuss the various effects of the selective packet drop attack on MANETs and to discuss various existing methods for detection of selective packet drop attack in MANETs. After study of various effects of the selective packet drop attack on MANET, to propose a new mechanism for detection and isolation of Selective Packet Drop attack in MANET while improving the performance of the network in terms of throughput, packet loss, delay, and overhead. The proposed technique also needs to be simulated by using AODV in NS-2 Simulator.

3. RELATED WORK

Subsequent section contains the detail study of different techniques, especially designed for detecting the selective packet drop attack. The main objective of this study is to evaluate the shortcomings of existing techniques.

Diffie et al. [1] demonstrated a novel mechanism based on cryptography for secure communication in the network. In this approach, theories of computation and communication are used to solve cryptographic problems in the network. The Authenticated key exchange method is used for secure data transmission between the source and destination. Goel et al. [2] have proposed a novel technique for preventing the MANETs against selective packet dropping malicious nodes by using introducing the monitoring node concept. The proposed technique increases the performance in the terms of throughput and packet loss. Dilli, R. et al. [3] in their paper proposed a Secured

hash-based technique for secured routing in MANETs. The HMAC based technique is used for maintaining data integrity. The drawback of this technique is increased end-to-end delay. Patolia et al. [4] presented a new approach based on key exchange and monitoring (KEAM) to isolate malicious nodes from the network. This technique works on the basis of Diffie- Hellman key exchange method. The simulation results proved that performance of network is enhanced in the terms of throughput and end- to- end delay. Stulman et al. [5] make use of the handshake method of secure key exchange during communication between various nodes in MANETs. The advantage of using this approach is that there is no need of prior knowledge about the network to implement this technique for isolation of selective packet dropping attack. Arya et al. [6] have introduced a novel technique for detection of selective packet dropping attack in MANETs. The modified performance of AODV protocol has shown improved performance of Adhoc networks in the terms of packet delivery ratio and throughput. Anita et al. [7] have utilized the concept of Diffie- Hellman to detect selective packet dropping nodes in the MANETs. This technique removes the packet dropping problem in the network by improving the performance of the network in the terms of increased throughput.

Cho et al. [8] in their work present a source level trust-based mechanism for isolating selective packet dropping attack in Wireless sensor networks (WSNs). This mechanism proves the better performance of the network as compare to the beta and entropy based trust model for isolating the selective packet forwarding attack in WSNs. Minakshi et al. [9] in their work make use of HMAC-MD6 for securing AODV in MANET. This mechanism improves the authentication and integrity of the network. Kumar et al. [10] in their paper presented a mechanism which is based on the HMAC for secure data transmission in the MANETs. This mechanism works on the basis of secret key exchange between source and destination for secure data transmission. The method of encryption and decryption is used for securing the Adhoc network against packet dropping problems. Liao et al. [11] demonstrated a novel continuous monitor-forward based mechanism for prevention from selective packet dropping problem in MANETs. This trust-based mechanism is used for improving the network performance in the terms of reduced false positive rates. Vadhana et al. [12] have proposed an Ant based technique for prevention of selective packet dropping problem in MANETs. In this technique, S-ACK (Secure Acknowledgement) is transmitted in the network through forward ant agents. Backward ant agents are used for sending acknowledgement back to the source. In this way, secure path is established from source to destination in MANETs. The drawback of this approach is increased packet delay. Mohanpriya et al. [13] proposed a modified dynamic source routing (DSR) protocol for isolating selective packet dropping nodes from the ad hoc network. This modified DSR protocol detects the abnormal behavior of the attacker nodes in the network. If attacker nodes are part of the network, then these nodes are isolated by broadcasting Block messages in the network. Singh et al. [14] demonstrated a novel security enhanced zone routing protocol for securing routing packet in MANETs. This approach utilizes the message authentication code for maintaining the security policy of the network. The overhead of the network is reduced by implementing this approach. Ravilla et al. [15] provide a security mechanism based on message authentication code for MANETs. This

mechanism is introduced to hybrid routing protocol in MANETs for maintaining the data integrity.

Baadache et al. [16] provide the Merkle-tree mechanism based technique for preventing the ad hoc network from packet dropping attacker nodes. The results have shown improved detection and prevention rate as compare to watchdog and 2-hop ACK techniques used for multi- hop ad-hoc networks. Hao et al. [17] make use of game theory approach for isolating selective packet dropping nodes from the MANETs. This technique can also be used for prevention from collaborative attacker nodes, which collectively launch an attack on the ad hoc network. Ming [18] introduced a new approach to mitigating selective packet drop attack in MANETs. In this approach, number of IDS nodes are used for detection of malicious nodes. All of the nodes are set in sniffing mode, which continuously monitor the performance of all of the nodes in the network. If any suspicious node exceeds the predefined threshold, then a block message is broadcasted on the network for isolating attacker nodes. In this approach, false positive rates are reduced. The drawback of this approach is increased packet delay. Chuachan et al. [19] have utilized the challenge and response scheme for preventing the MANETs from selective packet dropping attacker nodes. This scheme is responsible for effectively detecting the packet dropping nodes in the networks. The network overhead is increased by using this approach. Shaw et al. [20] proposed a Deoxyribonucleic acid (DNA) based approach to preventing the network from malicious nodes. In this approach, Hash Message Authentication code is used for securing the Adhoc network. In this mechanism, there is no need of prior knowledge about the networking nodes. This technique also works when there is no knowledge of public keys in the network. Venkatesham et al. [21] have utilized the concept of Diffie-Hellman for resolving security issues of MANETs. This key exchange mechanism is used for maintaining the confidentiality and authenticity of the network.

Xiaoa et al. [22] make use of checkpoint based acknowledgment approach for preventing MANETs against selective packet drop problem in MANETs. In this technique, checkpoint nodes are elected from the intermediate nodes for checking the activities of other nodes in the network. By using this technique, the overhead of the network can be reduced. Ravilla et al. [23] have utilized the concept of hash algorithms for improving the security in MANETs. This approach increases the performance in terms of throughput and packet delivery ratio. The drawback of this approach is increased end to end delay. Zhou et al. [24] have introduced a novel hybrid key establishment mechanism for securing MANET. In this mechanism, the whole network is divided into parts as cell groups and cell controls. The public key encryption policy is adopted to maintain the security policy of the data packets in the network. Chauhan et al. [25] presented a novel approach for securing MANETs by using key management and routing mechanism. In this approach, the whole network is divided into different groups with group leaders. It is the responsibility of group leaders to authenticate all of the nodes to maintain authenticity of the network. Gurung et al. [26] provide a mechanism for mitigating Gray hole attack in MANETs. In this mechanism, monitoring nodes are used for watching the performance of neighboring nodes. If the value of the packet dropping value of any node crosses the predefined threshold, then an alarm

message is broadcasted on the network for isolating that attacker node from the network. By using this mechanism, the performance of MANETs is increased in the terms of throughput and overhead.

From the literature survey, it is clear that Diffie- Hellman and HMAC based approaches are best suited for detecting selective packet drop attack in MANETs. But both of these techniques have a number of drawbacks. These drawbacks can be removed by using both of techniques collectively for detecting and isolating selective packet dropping nodes from the MANET. As the Diffie- Hellman based approach uses the asymmetric key, which slow down the encryption and cannot be efficiently used for the bulk of encryptions for each node separately. This drawback is removed by using an HMAC based approach for the rest of the operation which is fast as compare to Diffie- Hellman. The Diffie- Hellman works on the principle of man in the middle based approach, so it is not capable of authenticating each node involved in the network. To remove this drawback, it is collaborated with the HMAC based approach. Both of these techniques are used collectively for mutual authentication and maintaining the data integrity. As the HMAC based technique works on the basis of a shared secret key, so the hybrid technique is used for maintaining the perfect forward secrecy without depending on the public key infrastructure alone. The message digest functions used for HMAC are much faster to calculate than the symmetric key cryptographic functions used in Diffie-Hellman approach. The HMAC functions can be used for real-time applications. These functions are very small as compare to digital signatures but provide comparable security. For identifying the insecure path between the source and destination node, Diffie- Hellman approach is used as compared to HMAC function, because by using the HMAC function if shared key between both of the parties is compromised, then an attacker can create fraudulent messages. The advantage of the Diffie- Hellman approach is not limited to the two users, it means it can work for the open multiuser environment. It can also work where there is no prior knowledge of nodes in the network. The Diffie- Hellman approach is safely used for detecting the insecure channel because, in this approach, there is no need to share a secret key within the nodes. The main drawback of the Diffie- Hellman approach is its slow speed. The speed of the whole process of detecting and isolating selective packet drop attacker nodes from the MANET is increased by collaborating it with the HMAC based approach. The drawback of the Diffie- Hellman approach is that any intermediate node can exchange the key and listen to the communication between the source and destination nodes. This method cannot be used efficiently for encrypting the messages, so it is best suited for checking whether path is secured or not. The hash function works on the basis of shared secret key, so it is preferred to use this function with the monitor nodes. The Diffie-Hellman approach is used in conjunction with HMAC to make it more secure. There are various drawbacks of both of the techniques, so it is better to use DHHP technique which uses both the qualities of two different techniques for better detection and isolation of malicious nodes in the MANET.

4. PROPOSED DESIGN

The proposed mechanism is used to detect and isolate the selective packet drop attack in MANET for improving the performance of the network by using DHHP approach. The whole concept for detection and isolation depends upon the two different techniques.

a) Diffie- Hellman for finding a secure path from source to destination in MANET.

b) HMAC technique for isolation of malicious nodes from the MANET.

4.1 Diffie- Hellman Technique

The mobile Adhoc network can be created by taking finite number of nodes. The Diffie-Hellman technique is used to check whether a path is secure or not. In the MANET, find the source and destination nodes, which want to communicate with each other for transferring the data packets. For finding the shortest path between these nodes, AODV routing protocol is called. All of the nodes in the path from source to destination will reply with their hop count and sequence number. A path with the minimum hop count and maximum sequence number will be selected as the shortest path from source to destination, but this path needs not to be the secured path. For verifying this path Diffie-Hellman algorithm is used.

In this mechanism, first of all, a channel from source to destination is established. After this, communication is started for transferring the data packets. In Diffie- Hellman based approach, nodes at the source and destination will generate two random numbers p (prime number) and b (base number). After this, private key S_k at the source node and private key D_k at the destination node are generated. From these values, two values X and Y are calculated on the source and destination ends respectively by using the following formulas

$$X = b^{Sk} \text{mod} p \quad \ldots\ldots\ldots\ldots\ldots (1)$$

$$Y = b^{Dk} \text{mod} p \quad \ldots\ldots\ldots\ldots\ldots (2)$$

Both of the nodes exchange these values of ‘X’ and ‘Y’ with each other for calculating the secret key value ‘Z’ at the both ends. The formulas for calculating secret key value at the source and destination nodes respectively are

$$Z_S = Y^{Sk} \text{mod} p \quad \ldots\ldots\ldots\ldots\ldots (3)$$

$$Z_D = X^{Dk} \text{mod} p \quad \ldots\ldots\ldots\ldots\ldots (4)$$

These values of secret keys are exchanged with each other for checking whether equal or not. If values are identified as equal at both source and destination, it means channel is secured for communication. Otherwise, there will be some malicious nodes in the network, which are dropping packets on the way from source to destination. The flow chart shown in figure 3 represents the Diffie-Hellman approach for checking the path.

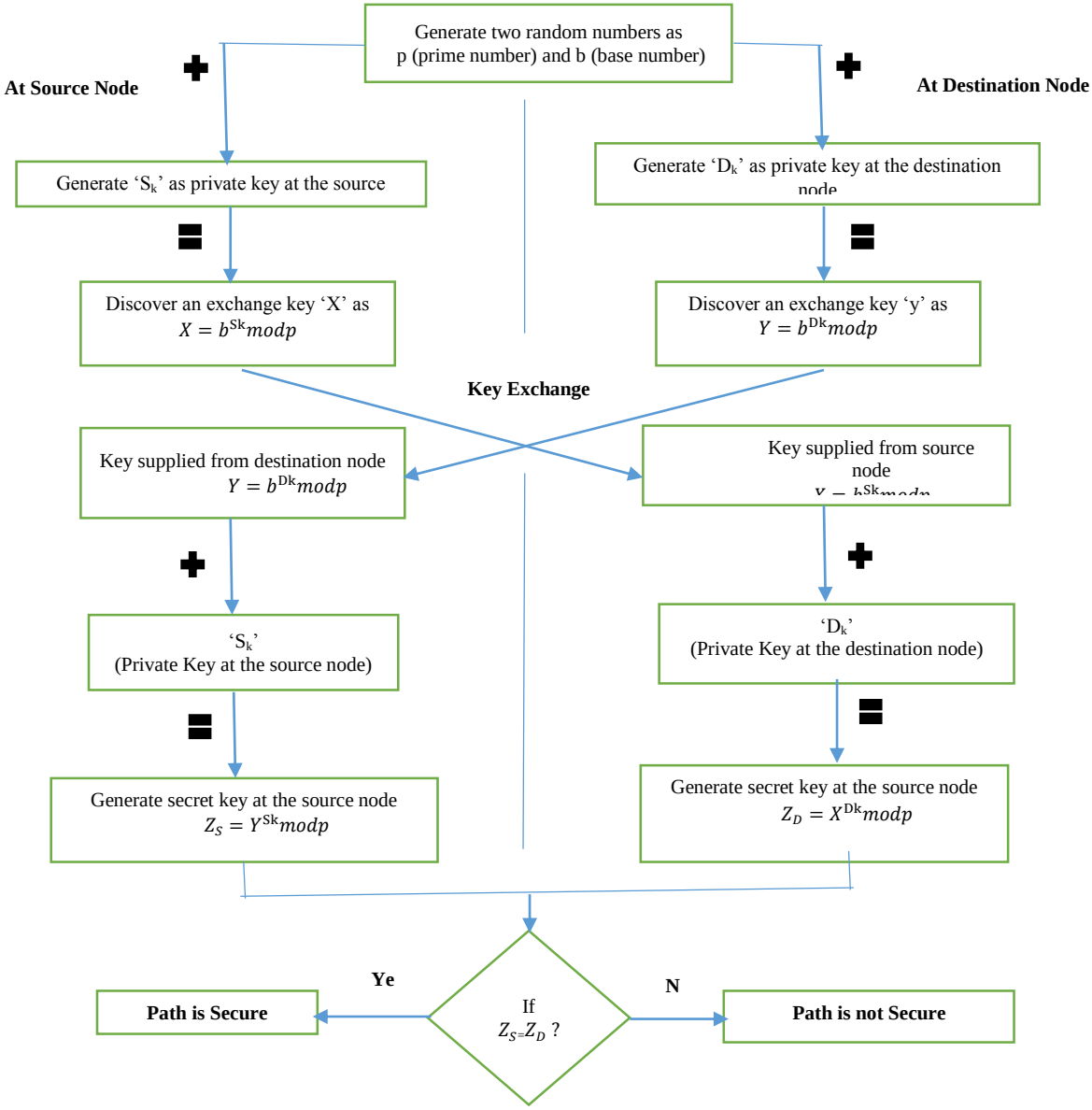

Figure 3. Diffie-Hellman approach for checking whether path is secure or not

4.2 HMAC Technique

After detecting the insecure path by using a Diffie-Hellman technique, the next process is to detect and isolate particular malicious nodes from the network. For this task, HMAC (Hashed message authentication code) based technique is adopted. In this approach, a central network administrator is used for setting all of the nodes in the network to the monitor mode. All of these nodes will watch the performance of each node in the path from source to destination. These nodes will check the packet receiving and the packet forwarding ratio of each node in the insecure path. In this approach,

HMAC function is used to locate the malicious nodes in the network, which are selectively dropping the data packets. All of the nodes in the insecure path from source to destination will be selected in sequence as an intermediate node between the same source and destination. The other nodes will act as monitor nodes for checking the performance of nodes which lies in the path from source to destination. In HMAC based technique, both Source and destination nodes shared a secret key with each other for encryption and decryption. All of these nodes are individually checked by monitor nodes in the network. This process of monitoring is accomplished by using HMAC based approach. The whole process of monitoring the nodes in the insecure path is shown in the figure 4.

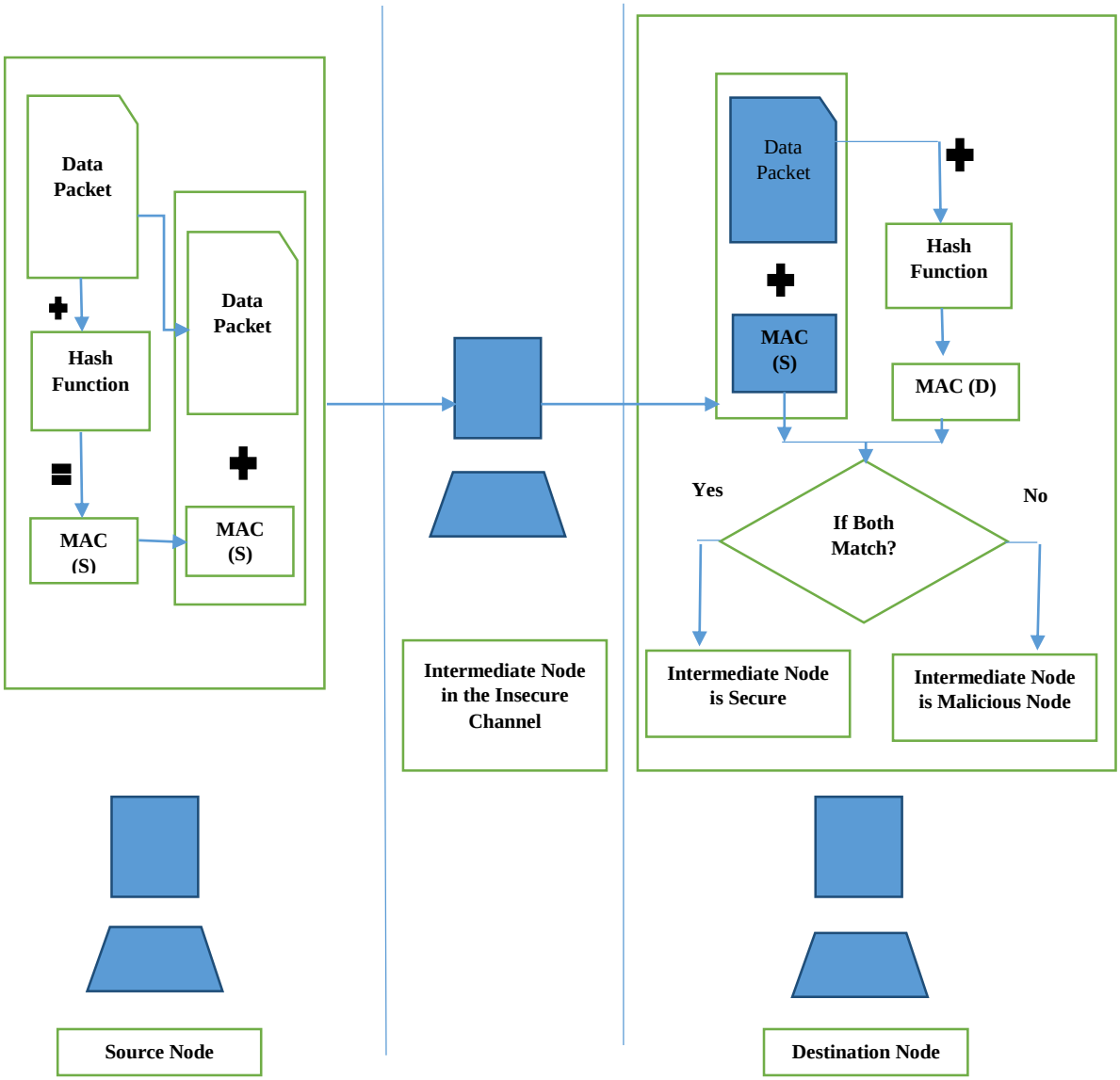

Figure 4. HMAC based approach for detecting malicious node in MANET.

In this approach, for isolating the malicious node from the MANET, First of all, one

node is selected from the insecure path towards the destination node. After selecting the particular node, hash function is applied to the data packets at the source for obtaining MAC at the source node. This MAC and data packet transfer through an intermediate which is part of the nodes in the insecure channel. At the destination node, again same hash function is applied to the received data packet for obtaining new MAC. If MAC received from the source and MAC generated at the destination, both match with each other. It means path from source to destination through the particular node is secure, then another node from the insecure channel will be selected as an intermediate node from source to destination. In another condition, if both MAC does not match at the destination node. It means path through the particular node is not secured and this node needs to be isolated from the network. For isolating this node from the network, the central network administrator will broadcast a block message in the network, for isolating the particular node from the network. In this way, malicious node which is selectively dropping the data packets are isolated from the MANET. The whole process of detecting and isolating the malicious nodes from the network by using a hybrid technique is shown in the following figure.

By using an HMAC based approach, the source node Message Authentication Code (MAC) is generated by encrypting messages with secret key using Hash function. The original message and MAC are transferred collectively through insecure channel and performance of each of the nodes in this channel is monitored by all of the monitoring nodes. At the destination again hash function is used to decrypt the data by using a secret key. The hash function is utilized to obtain the MAC from the message received by using the shared secret key. This MAC is compared with the MAC received along with the message at the destination. If both of these MAC does not match, it means the node through which data is obtained is selective dropping the packets. The monitoring node will inform the central network administrator for isolating this malicious node from the network. The central network administrator will broadcast the message in the MANET for isolating that malicious node from the network.

When this node is isolated, then the next best path from the stored paths by AODV protocol is selected. This process of Diffie- Hellman is again repeated to get the secure path from source to destination node. If the keys match at both of the ends, it means the path is secured and data will be transferred through that path. If the keys do not match, it means there will be some malicious nodes which need to be isolated by using HMAC technique and the same process will be repeated to remove the malicious node and to establish a new secured path from source to destination. This process will be repeated until a secured channel is established from source to destination. In this way, the properties of both of the algorithms are utilized to improve the performance of MANETs under the AODV protocol. By using this hybrid technique, drawbacks of both existing techniques are also overcome. The working of DHHP is clearly depicted in the Figure 5.

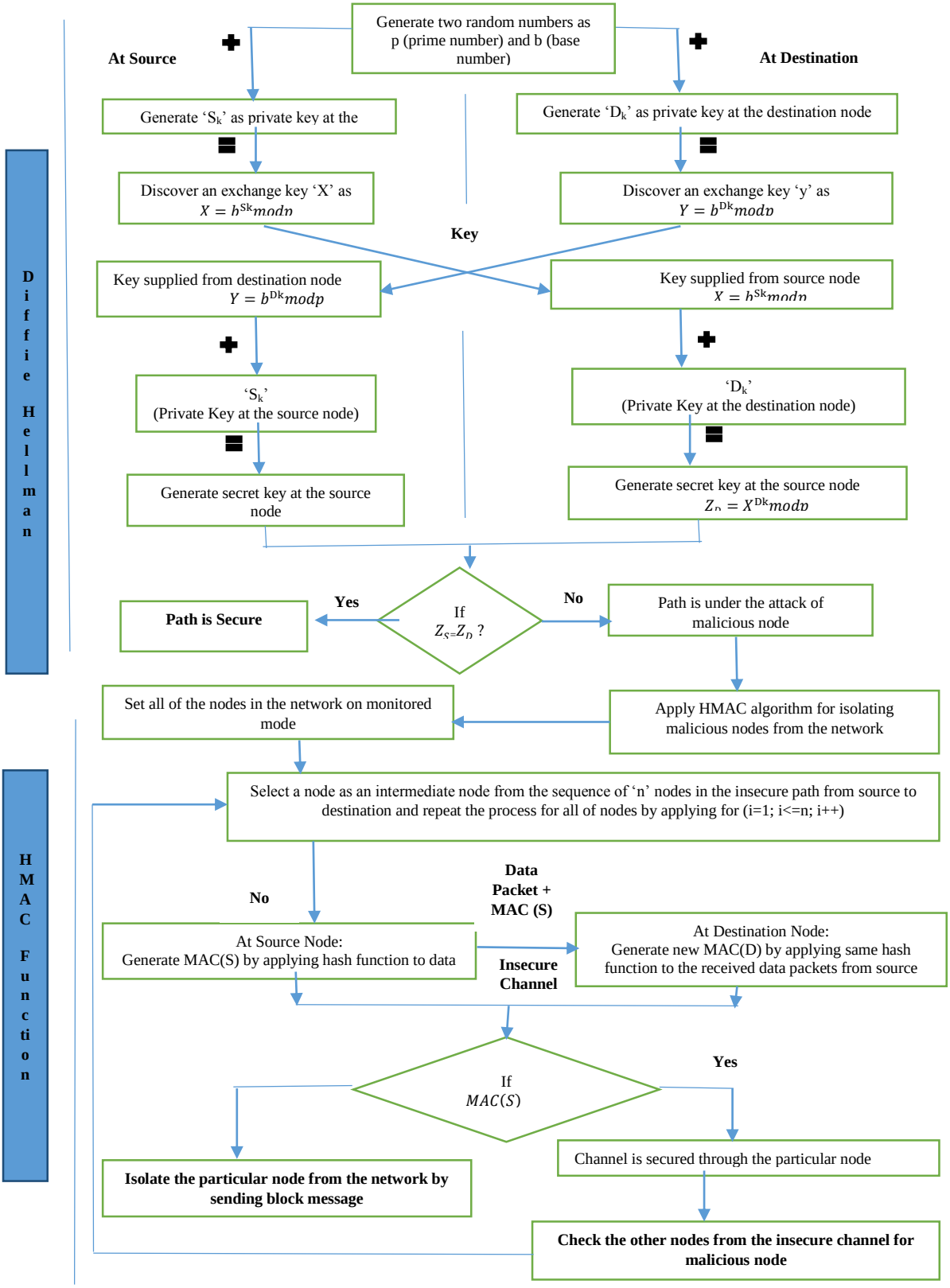

Figure 5: Flowchart showing the proposed DHHP for isolating malicious node

5. EXPERIMENTAL SETUP AND RESULTS

The NS 2.3 simulator is used for checking the efficiency of proposed hybrid technique for MANET. The proposed technique for prevention against selective packet drop attack is implemented on the Linux workstation (2.4 GHz Intel i3 processor with 2 GB RAM). The network is simulated by using 23 nodes. The various simulation parameters are presented in Table 1.

Table 1: Simulation Parameters

Parameter	**Value**
Simulator	NS 2.3
Duration of Simulation	600 seconds
Dimensions	800X800 (meters)
Adhoc nodes	23
Protocol	AODV
Communication type	Adhoc Network
Size of Packet	1024 Kilo Bytes
Model	Two ray ground propagation model

The simulation of the proposed technique is performed by deploying the MANET by using NS2.3 simulator. In this network, node 0 is the source node and node 10 is the destination node. The node 0 floods the route request in the network for getting path to the destination node 10. The various nodes in the network reply with best path towards destination. A source node will select the shortest path towards the destination as shown in the figure 6 without considering malicious node in the network. First of all, Diffie- Hellman technique is used for checking whether the route is under the attack of malicious nodes or not. By applying the proposed technique if the route from source to destination is not secured, then this route is rejected as shown in figure 7. The next step is to detect and isolate that malicious node from the MANET. After detecting the unsecured path from source to destination, the whole of the network is set into monitoring mode by using the HMAC function as shown in the figure 8. For this operation, central network administrator is used. All of the nodes in the MANET watch the performance of their neighboring nodes under some predefined parameters. If the input and output values of a node in the path are different, then this node is considered as a malicious node which are selectively dropping the data packets as

shown in the figure 9. The information about this node is forwarded to a central network administrator by monitoring nodes. The central network administrator will broadcast a message to isolate that malicious node from the network. After this, the next best path is selected from source to destination which does not include that malicious node. The whole process mentioned above is again followed to isolate malicious node if exists in the path. This process is repeated until a secured path is found out. At the last data is transferred through that secured path. The figure 10 represents the safe path from source to destination by isolating selectively packet dropping nodes. In the next section of the paper, the performance of the proposed technique is measured against various parameters.

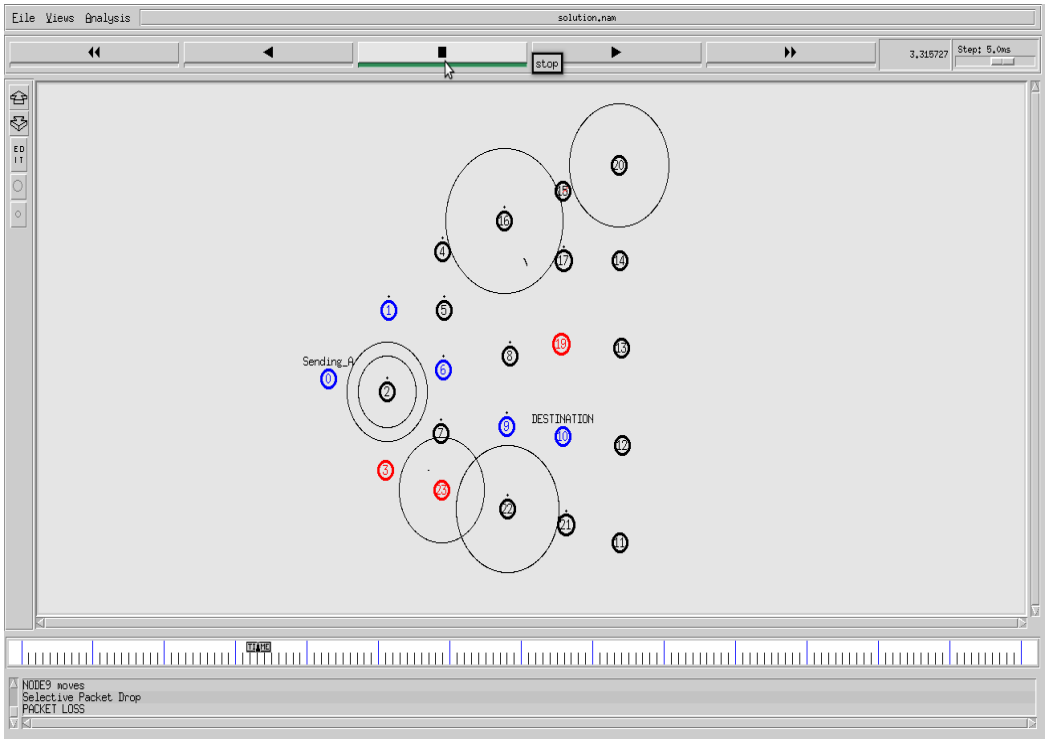

Figure 6: Route discovery in adhoc network

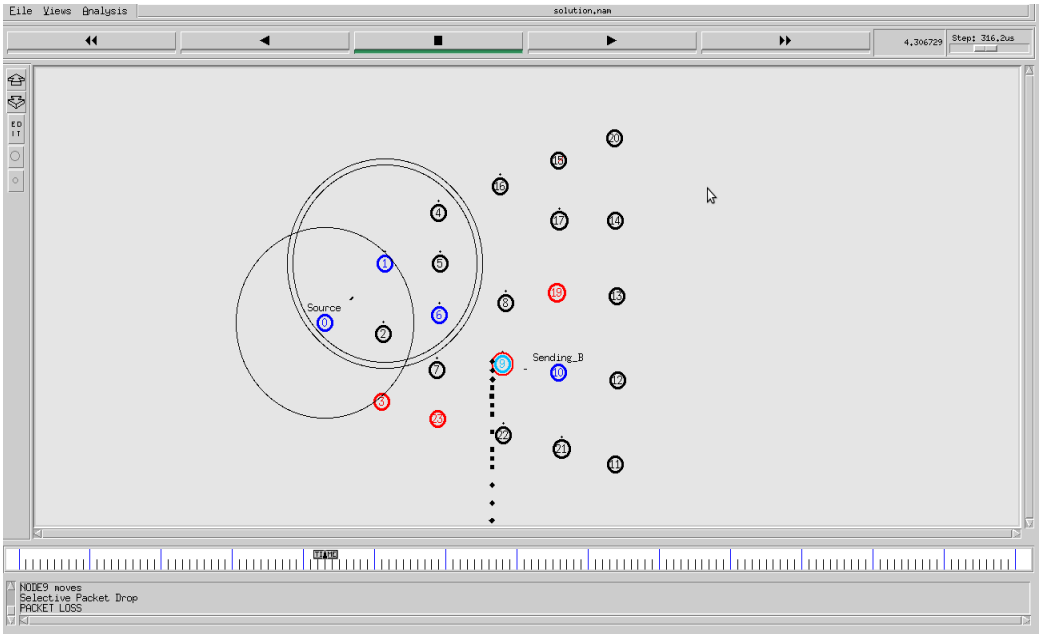

Figure 7: Malicious node selectively dropping the data packets

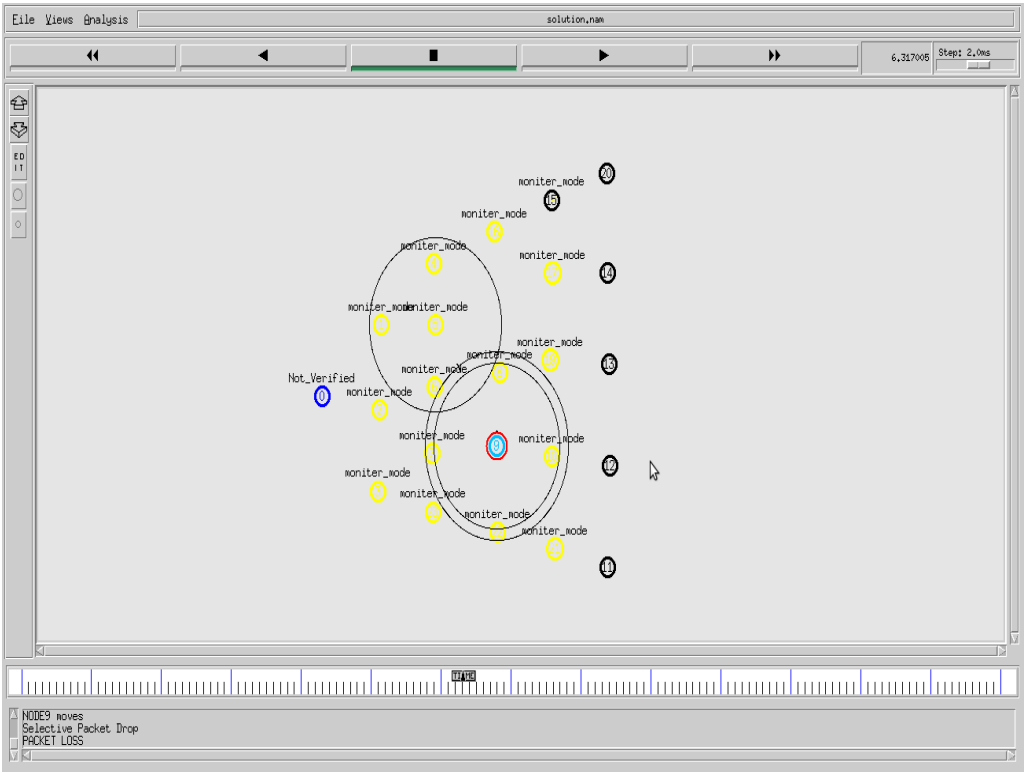

Figure 8: Nodes in monitoring mode for detecting malicious nodes

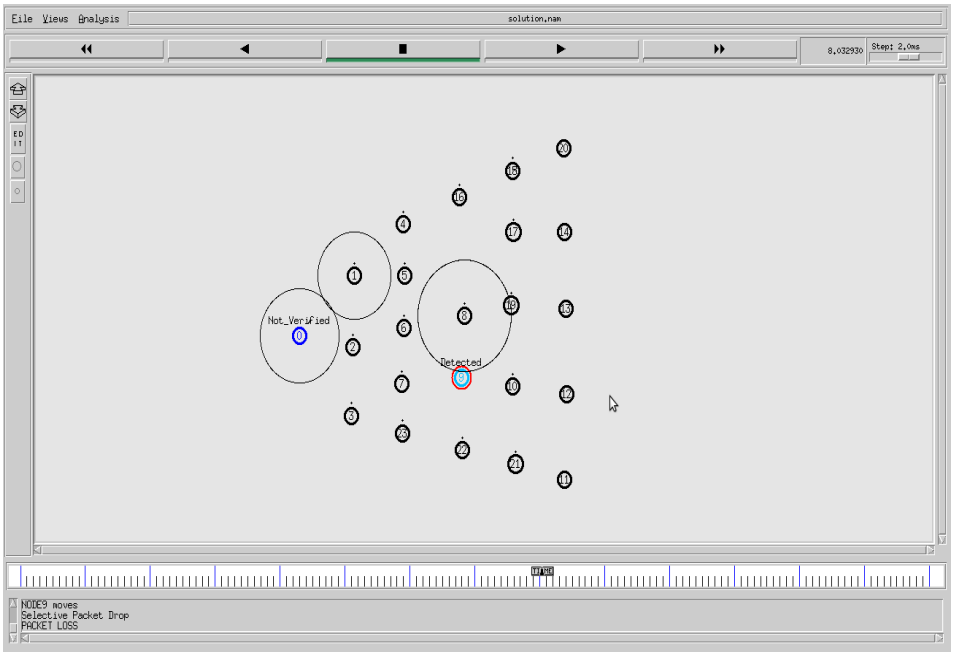

Figure 9: Malicious node detected by monitoring nodes

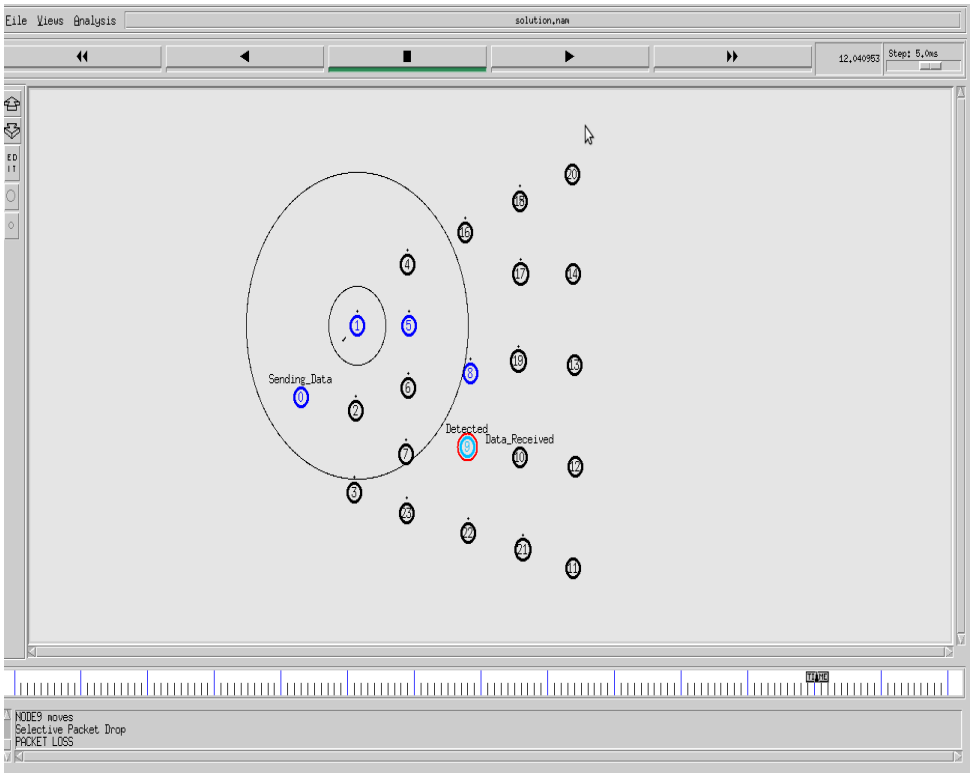

Figure 10: Secure path by isolating malicious node

5. PERFORMANCE ANALYSIS

This section presents the performance of the DHHP technique under various parameters. The Throughput, Delay and Packet loss are basic parameters for measuring the performance of Adhoc networks. The throughput represents the total number of successfully delivered data packets. The value of this parameter can be increased if malicious node is detected as soon as possible. The throughput is calculated as

$$\text{Throughput} = \frac{\Sigma M}{T} \ldots\ldots\ldots\ldots\ldots\ldots (5)$$

Where

M=No. of messages successfully reached on the destination,

T=Simulation time

Figure 11 depicts the increased throughput of the network after isolation of selective packet dropping attack as compared to the throughput of the MANET under the attack of malicious node.

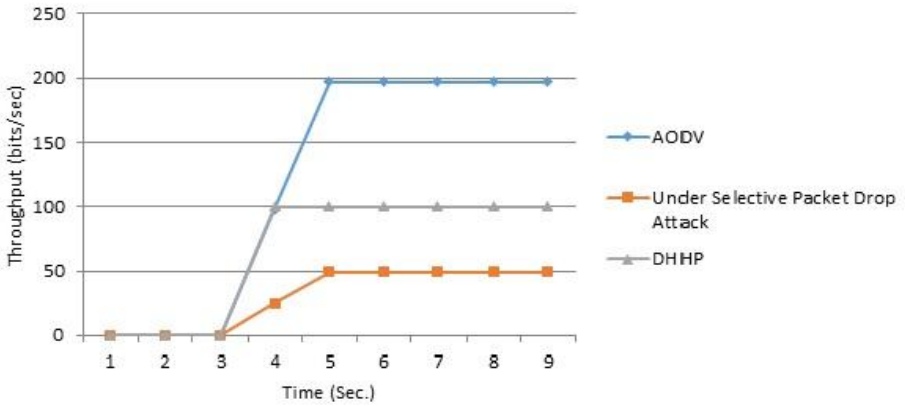

Figure 11: Increased throughput of the MANET by using hybrid technique

End-to–end delay represents the total time taken by a data packet to reach at the destination. The delay includes the time taken during the route discovery process and to travel the data packets from source node to the destination node. In this parameter, only those data packets are considered which are successfully delivered at destination. End- to-end delay is calculated as

$$\text{Delay}=\frac{\Sigma(A-S)}{\Sigma(N)} \ldots\ldots\ldots\ldots\ldots\ldots (6)$$

Where

A =Value of Time when the data packet reaches at the destination,

S =Initial time of route discovery process,

N = Number of Connections

The decreased value of the end-to-end delay in figure 12 indicates the improved performance of proposed hybrid technique. The figure depicts that the hybrid technique, decrease the value of end-to-end delay as compared to MANET under the attack of malicious node.

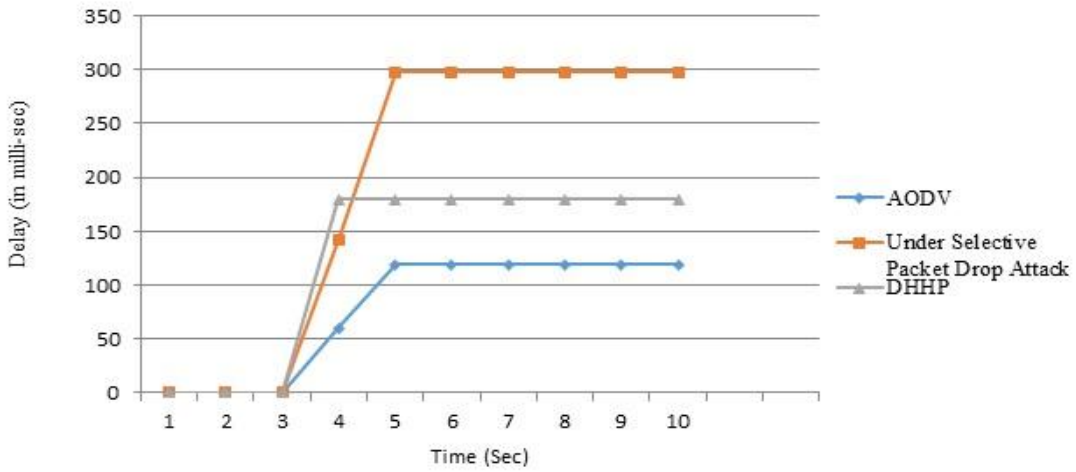

Figure 12: Decreased delay of the MANET by using hybrid technique

The packet loss is the measure of the total number of packets failed to reach at the destination. This happens due to the presence of malicious node or congestion in the network. The value of the packet delivery ratio parameter decreases with increase of packet loss. The value of this parameter is calculated as

$$\text{Packet Loss} = \eta - \delta \quad \ldots\ldots\ldots\ldots (7)$$

Where

η = Total number of data packets sent from the source node

δ = Total number of data packets reached at the destination node

Figure 13 clearly depicts the decreased packet loss by implementing the proposed technique as compare to MANET under the attack of malicious node.

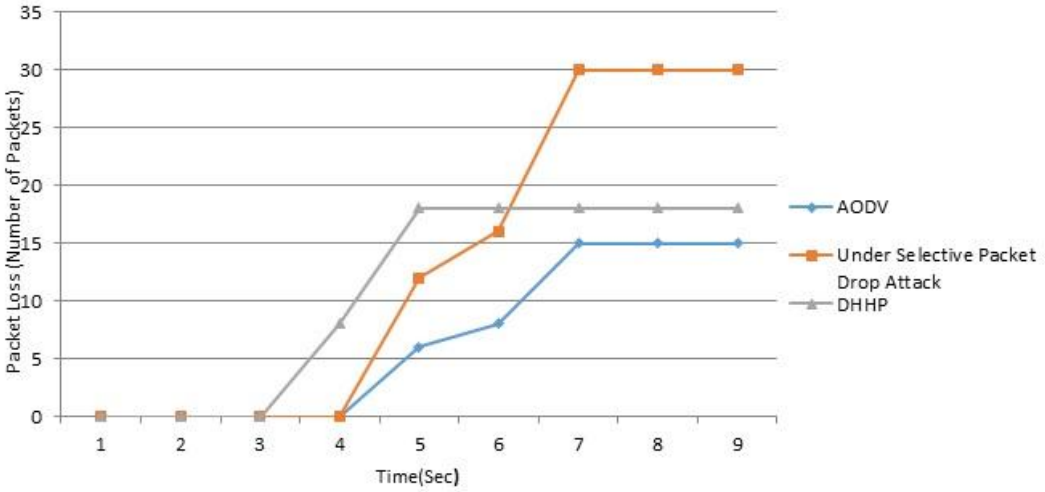

Figure 13: Decreased packet loss of the MANET by using hybrid technique

The overhead is measured as the additional time taken for delivering the data packets at the destination node. The malicious nodes in the network increase the overhead in the MANET. By implementing the proposed approach, the overhead of the network is decreased as compared to the MANET under the attack of malicious node. The figure 14 represents the decreased overhead after implementing the DHHP technique.

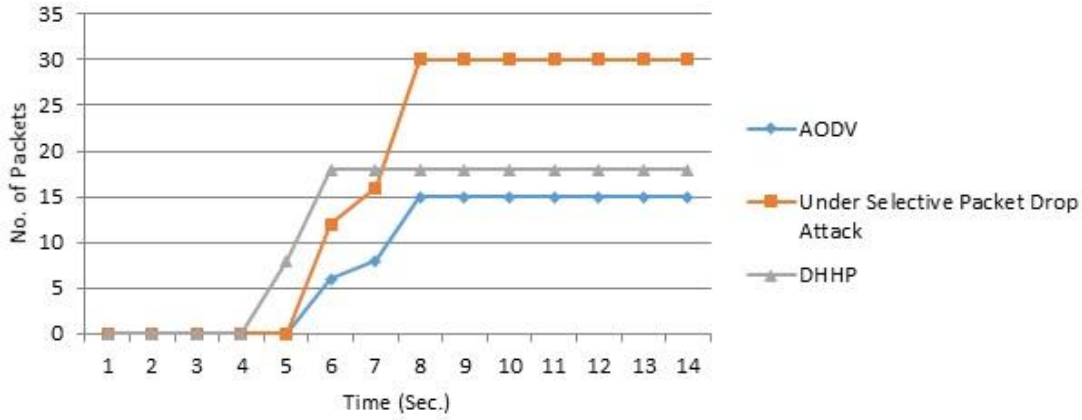

Figure 14: Decreased overhead of the MANET by using hybrid technique

6. CONCLUSION AND FUTURE WORK

The Selective packet drop is a very dangerous attack in MANETs, which is very difficult to detect and isolate. In this type of attack, the malicious node most of time behaves like a normal node and suddenly starts dropping packets. The selective packet

dropping nodes reduce the performance of the network in the terms of various parameters. In the literature, we have studied that the Diffie- Hellman and HMAC based approaches are mostly used for detecting and isolating selective packet dropping nodes in MANETs. There are various drawbacks of both of these techniques. In this work, we have proposed a new DHHP technique which removes the drawbacks of these techniques. The Diffie- Hellman technique is used to check whether the path from the source node to destination node is secure or not. If path is not secured, then HMAC is executed for detecting and isolating malicious node from the MANET. In HMAC based approach, all of the neighboring nodes of the insecure path are set to the monitor mode for checking the performances of the various nodes in the insecure channel. If any node found to be malicious, then a central network administrator will be used to flood block message in the network to isolate that node from the network. This hybrid technique is designed and implemented with NS 2.3 simulator. The experimental results clearly shown the improved performance of the MANET in the terms of throughput, overhead, delay and packet loss. In future, this hybrid technique can be extended for some other protocols. The same approach can be used for tackling some other attacks in MANET. The concept of data mining can also be incorporated with this hybrid technique for differentiating various attacks.

ACKNOWLEDGEMENT

Authors are highly thankful to the Department of RIC, IKG Punjab Technical University, Kapurthala, Punjab, India for providing the opportunity to conduct this research work.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

REFERENCES

[1] Diffie, W. and Hellman, M., "New Directions in Cryptography", IEEE transactions on information theory, Vol. IT-22, No. 6, 1976.

[2] Goel, P. and Kumar, P., "Detection and isolation of selective packet drop attack in MANET using Diffie - Hellman algorithm", International Journal of Latest Research in Science and Technology, Vol. 3, Issue 3: pp. 137-139, 2014.

[3] Dilli, R., Reddy, P., "Implementation of Security features in MANETs using SHA-3 Standard Algorithm", International Conference on Computational Systems and Information Systems for Sustainable Solutions, 2016.

[4] Patolia, S., Kumar, N., "KEAM- To Isolate and Prevent Selective Packet Drop Attack in MANET", International Journal of Innovative Research in Science, Engineering, and Technology, Vol. 4, Issue 5, 2015.

[5] Stulman, A.; Lahav, J. and Shmueli, A., "MANET Secure Key Exchange using Spraying Diffie-Hellman Algorithm", International Conference for Internet Technology and Secured Transactions", 2012.

[6] Arya, M. and Jain, Y., "Grayhole Attack and Prevention in Mobile Adhoc Network" in International Journal of Computer Applications, Vol. 27, No.10, 2011.

[7] Anita, Abhilasha, "A Novel Technique to Protect and Isolate Selective Packet Drop Attack in MANET", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 6, 2014.

[8] Cho, Y. and Qu, G., "Detection and Prevention of Selective Forwarding-Based Denial-of-Service Attacks in WSNs", in International Journal of Distributed Sensor Networks, Hindawi Publishing Corporation, 2013.

[9] Minakshi and Gill, R., "Secure AODV using HMAC-MD6 in MANET", International Journal of Computer Science & Management Studies, Vol. 13, Issue 09, 2013.

[10] Kumar, A., and Logashanmugam, E., "To Enhance Security Scheme for MANET using HMAC", International Conference on Current Trends in Engineering and Technology, 2014.

[11] Liao, H. and Ding, S., "Mixed and Continuous Strategy Monitor-Forward Game Based Selective Forwarding Solution in WSN", International Journal of Distributed Sensor Networks, Hindawi Publishing Corporation, 2015.

[12] Kumari, V. and Paramasivan, B., "Ant-based Defense Mechanism for Selective Forwarding Attack in MANET", IEEE International Conference on Data Engineering Workshops (ICDEW), 2015.

[13] Mohana Priya, M. and Krishna murthi, I., "Modified DSR protocol for detection and removal of selective black hole attack in MANET" in Computers and Electrical Engineering, Elsevier, 2013.

[14] Singh, S. and Trivedi, M., "Securing Zone Routing Protocol in MANET using Authentication Technique" in International Conference on Computational Intelligence and Communication Networks, 2014.

[15] Ravilla, D. and Reddy, C., "Implementation of HMAC-SHA256 Algorithm for Hybrid Routing Protocols in MANETs", International Conference on Electronic Design, Computer Networks & Automated Verification (EDCAV), 2015.

[16] Baadache, A. and Belmehdi, A., "Fighting against packet dropping misbehavior in multi-hop wireless ad-hoc networks" in Journal of Network and Computer Applications, Elsevier, vol. 35, pp. 1130-1139, 2012.

[17] Hao, D.; Liao, X.; Adhikari, A.; Sakurai, K. and Yokoo, M., "A repeated game approach for analyzing the collusion on selective forwarding in a multihop wireless networks", Computer Communication, Elsevier, vol. 35, pp. 2125-2137, 2012.

[18] Su, M., "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Computer Communications, Elsevier, vol. 34, pp. 107–117, 2011.

[19] Chuachan, T.; Puangpronpitag, S., "A Novel Challenge & Response Scheme against Selective Forwarding Attacks in MANETs", International Conference on Ubiquitous and Future Networks (ICUFN), 2013.

[20] Shaw, H.; Hussein, S. and Helgert, H., "Prototype Genomics-Based keyed-Hash Message Authentication Code Protocol", International Conference on Evolving Internet, 2010.

[21] Venkatesham, T. and Satyanna, K., "Diffie-Hellman Key Exchange Mechanism to Provide Secured Communication in Manet", in International Journal of computer science and Electronics Engineering, Vol.4, Issue.5, 2014, page No. 56-62.

[22] Xiaoa, B.; Yua, B. and Gao, C., "CHEMAS: Identify suspect nodes in selective forwarding attacks", Journal of Parallel and Distributed Computing, Elsevier, pp. 1218-30, 2007.

[23] Ravilla, D. and Reddy, C., "Enhancing the Security of MANETs Using Hash Algorithms", in International Multi-Conference on Information Processing (IMCIP), science direct, 2015.

[24] Zhou, H., Zheng, M. and Wang, T., "A Novel Group Key Establishment Scheme for MANETs" in Advanced in Control Engineering and Information Science, science direct, 2011.

[25] Chauhan, K. and Sanger, A., "Securing Mobile Ad hoc Networks: Keys Management and Routing", in International Journal on Adhoc Networking Systems (IJANS), Vol. 2, No. 2, 2012.

[26] Gurung, S. and Chauhan, S., "A novel approach for mitigating gray hole attack in MANET" in Wireless Networks, Springer Science, and Business Media, 2016.