Enhanced Intrusion Detection System with On-Demand Routing Protocol using Hybrid Cryptographic Technique for MANETs

Avinab Marahatta, Kare Suresh Babu

Abstract— The migration to wireless network from wired network has been a global trend in the past few years. The scalability and mobility brought by wireless network made it possible in many applications. Among all the up to date wireless networks, Mobile circumstantial Network (MANET) is one amongst the foremost necessary and distinctive applications. On the contrary to ancient spec, MANET doesn't need a set network infrastructure; each single node works as a transmitter and a receiver and they trust their neighbors to relay messages. Nodes communicate directly with each other when they are both within the same transmission range. Or else, they rely on their neighbors to relay messages. Self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and remote distribution of MANET create it at risk of numerous kinds of attacks. Therefore it is very crucial to develop efficient intrusion detection mechanisms to protect MANET from attacks. In this paper, we define solid privacy requirements regarding malicious attackers in Mobile Ad-hoc Network. We propose and implement a new intrusion detection system named Enhanced Intrusion Detection System with On-Demand Routing Protocol using Hybrid Cryptographic Techniques for MANETs. Compared to contemporary approaches, it demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

Index Terms— AACK, ACK , EAACK, Hybrid Cryptography, IDS, MANET , TWOACK

1 INTRODUCTION

The increasing demand of wireless communication and the needs of new wireless devices have tend to research on self configuring, self healing networks without the interference of centralized or pre-established infrastructure/authority. Networks with the absence of any centralized or pre-established infrastructure are called Ad hoc networks [6], [12], [31]. Ad hoc Networks are collection of self-governing mobile nodes.

Industrial remote access and control via wireless networks are becoming more and more popular these days. In the next generation of wireless network systems, there will be a need for the expeditious deployment of independent mobile users. Consequential examples include establishing survivable, effectual and dynamic communication for exigency/rescue operations, disaster mitigation efforts, and military networks. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. The communication is limited to the range of transmitters from one node to another. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own.

MANET solves this problem by allowing intermediate parties to relay data transmissions. It can be achieve by dividing MANET into two types of networks, which is single-hop network and multi hop network. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multi hop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their communication range. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly [4], [28]. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure. However, it is often infeasible in critical mission applications like military conflict or emergency recovery. Quick deployment and minimal configuration make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like military conflicts, medical emergency situations and natural or human-induced
disasters [19], [31].

Due to unique characteristics, MANET is becoming more and more widely implemented in the present scenarios[15], [29]. However, considering the fact that MANET is popular among critical mission applications where the network security is very important. Unfortunately, the remote distribution and open medium of MANET make it vulnerable to various types of attacks. As for example, due to the nodes' lack of physical protection, the malicious attackers can easily capture and compromise nodes to achieve attacks. While considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, any attackers can easily compromise MANETs by inserting malicious nodes into the network.

2 BACKGROUND

Missing a single component may significantly degrade the strength of the overall security solution. When more security features are introduced into the network in parallel with the

enhanced security strength is the communication and management overhead. The network performance, in terms of robustness, availability and scalability of the security solutions, becomes an important concern in ad-hoc network. Many contemporary proposals focus on the security vigor of their solutions from the cryptographic technique, people leave the network performance largely discourse. The dimensions of network performance and security strength are equally important. Achieving a good trade-off between two extremes is one fundamental challenge in security design for MANETs.

Nodes in MANETs assume that other nodes always cooperate with each other to relay data packet. The attackers with the opportunities to achieve significant impact on the network with just one or two malicious nodes. While solve this problem, the Intrusion Detection System should be added to enhance the security level of mobile ad-hoc networks. If the mobile ad-hoc networks can detect the attackers as soon as they enter the network to completely eliminate the potential damages caused by compromised nodes at first time only.

2.1 Watchdog

Watchdog aims is to improve the throughput of network with the presence of malicious nodes. The Watchdog is consisted of two parts, which are Watchdog and Pathrater. Where, Watchdog serves as IDS for MANETs. Watchdog is responsible for detecting malicious node misbehaviors in the network and detects the malicious misbehaviors by promiscuously listening to its next node transmission. The Watchdog node increases failure counter if it overhears that the next node fails to forward the packet within a certain period of time. If the node's failure counter exceeds a predefined threshold, then the Watchdog node reports it as misbehaving. In this situation, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission.

2.2 TWOACK

It detects misbehaving nodes or links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. When retrieval of a packet, each node along the route is required to send back an acknowledgement packet to the node that is two nodes away from it down the same route. The TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR), Ad-hoc On-Demand Distance Vector(AODV) routing protocol. The TWOACK successfully solves the receiver collision and limited transmission power problems posed by Watchdog intrusion detection system. However, the acknowledgement process required in every packet transmission process added a significant amount of unwanted network overhead.

2.3 AACK

It is an acknowledgement-based network layer scheme which can be considered as a combination of a TACK and ACK. Where TACK is identical to TWOACK and ACK is an end-to-end acknowledgement scheme called ACKnowledge(ACK). While compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. While considering the ACK scheme the source node S sends out Packet without any overhead. All the intermediate nodes need to forward this packet to the destination node. When the destination node D receives Packet, it is required to send back an ACK acknowledgement packet to the source node S along the reverse order of the same route. If the source node S receives this ACK acknowledgement packet within the predefined time, then the packet transmission from node S to node D is successful otherwise the source node S will switch to TACK scheme by sending out a TACK packet. This concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, even though both TWO ACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgement packets.

2.4 EAACK

In this EAACK system, there are different three approaches are implemented, namely, end to end acknowledgement scheme, secure acknowledgement scheme and misbehavior report authentication scheme. First it goes to ACK and forward the data packet from source to destination. If any malicious node found, it automatically goes to secure acknowledgement scheme which is identical to TWOACK. In secure acknowledgement mode the digital signature is implemented. Both the DSA and RSA algorithms used to generate the digital sign separately.

3 Problem Statement

Previous studies on Intrusion Detection System for MANETs focused more on only the data packet transmission and acknowledgement. There is no very secure intrusion detection system which not only deals about acknowledgement deals about the data packet encryption and transmission of data from one source to another destination. Moreover, the performance of different intrusion detection system had not been well measured since each researcher used different simulator and performance metrics for performance evaluation. Due to aforementioned problems there is continuous need to develop secure Intrusion detection system for MANETs. This proposed system is designed to tackle some of the weaknesses of Watchdog scheme, namely, limited transmission, false misbehavior, receiver collision and forge acknowledgement.

3.1 Receiver Collision

Receiver collision In the receiver collision problem as illustrated in the figure the node A can only identify whether node B has sent the data packet to node C, where node A cannot assure that node C has received it. If a collision occurs at node C when node B first forwards the packet, node A can only assume that node B has forwarded the packet and assumes that node C has successfully received it. Thus, B could skip retransmitting the packet and evade detection.

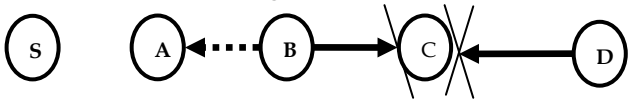

Fig. 1. Receiver Collision

In a typical example of receiver collisions, demonstrated in Fig. 2 after node A sends Packet1 to B node, it tries to overhear if node B forwarded this packet to node C; meanwhile, X node is forwarding packet2 to node C. In this situation, node A overhears that node B has successfully forwarded Packet1 to node C, but failed to detect that node C did not receive this packet due to a collision between Packet1 and Packet2 at node C.

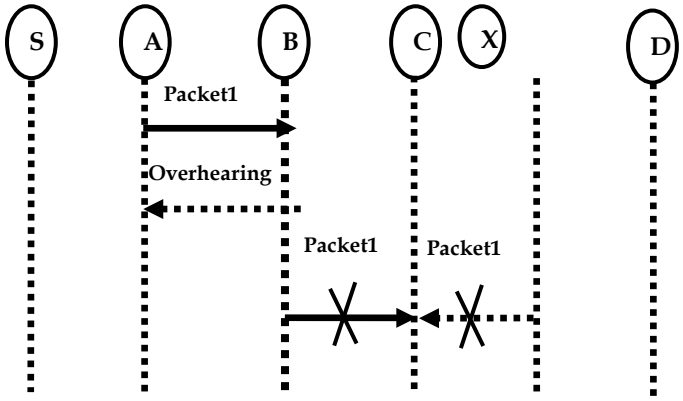

Fig.2. Receiver Collisions: Both node B and node X are trying to send packets to node C at the same time

3.2 Limited Transmission Power

In limited transmission power, node B intentionally limits its transmission power so that it is strong enough to be overheard by node A but not strong enough to be received by node C.

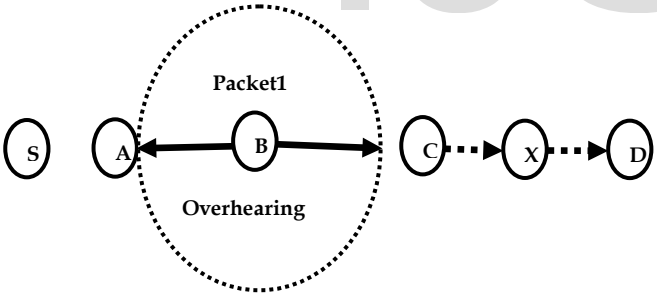

Fig.3 Limited Transmission Power

3.3 False Misbehavior

In false misbehavior report, although node A successfully overheard that node B forwarded Packet1 to node C, node A still reported node B as misbehaving, as shown in Fig.4. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack.

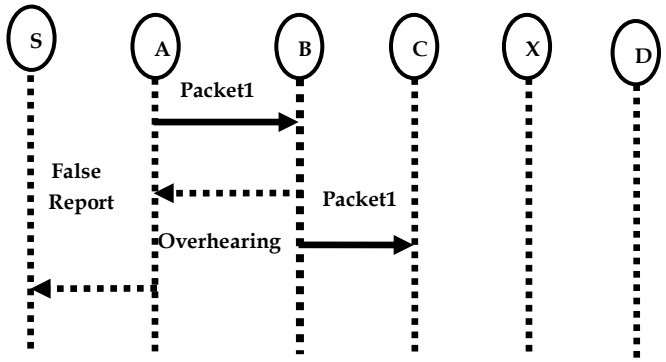

Fig.4. False Misbehavior Report

3.4 Forge Acknowledgement

In forge acknowledge, the node A successfully forwarded the data packet to the node B. Node B is sending acknowledgement to node A without forwarding data packet to node C.

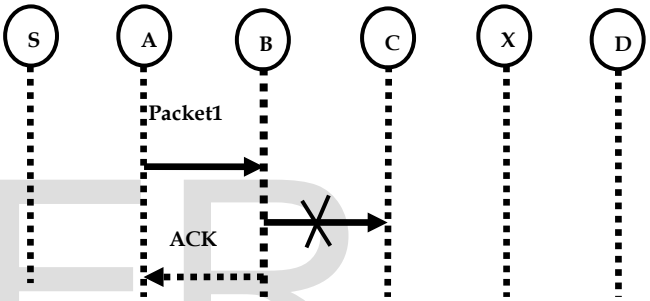

Fig.5. False Acknowledgement

4 PROJECT DESCRIPTION

In this proposed system, there are different approaches have implemented. First it goes to ACK. If any malicious node find, it automatically goes to S-ACK mode and goes for MRA scheme.

SOURCE TO DESTINATION NODE CONNECTION MODE

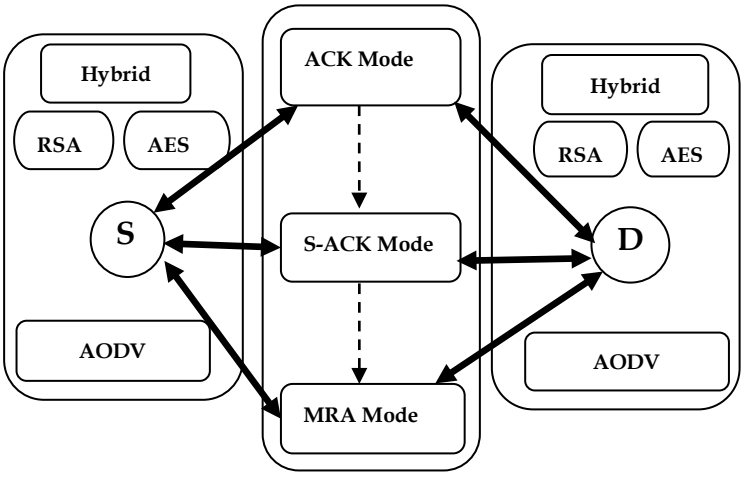

Fig.6. System Architecture

4.1 ACK Mode

While considering the ACK scheme the source node S sends out Packet without any overhead. All the intermediate nodes need to forward this packet to the destination node. When the destination node D receives Packet, it is required to send back an ACK acknowledgement packet to the source node S along the reverse order of the same route. If the source node S receives this ACK acknowledgement packet within the predefined time, then the packet transmission from node S to node D is successful otherwise the source node S will switch to Secure ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

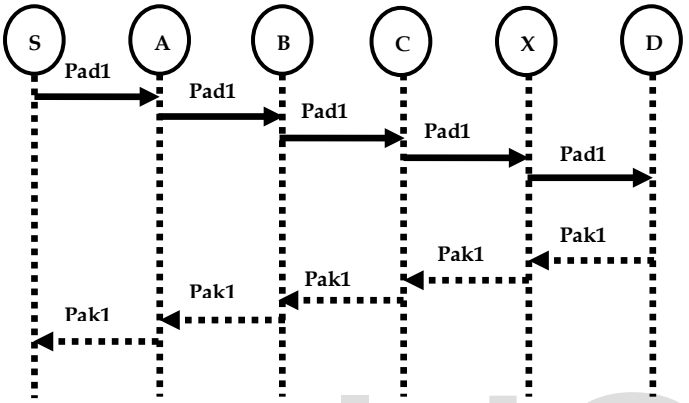

Fig.7. ACK Mode

4.2 S-ACK Mode

In S-ACK, the first node send out secure acknowledgement data packet to second node and same data packet forward to third node. When third node receives packet data, as it is the third node in this three node group, third node is required to send back an secure acknowledgement packet to second node. Second node forwards back to first node. If first node does not receive this acknowledgement packet within a predefined time period, both second and third nodes are reported as malicious node. A misbehavior report will be generated by first node and send to source node. Where the source node immediately trusts the misbehavior report, it requires the source node to switch to MRA scheme and confirm this misbehavior report.

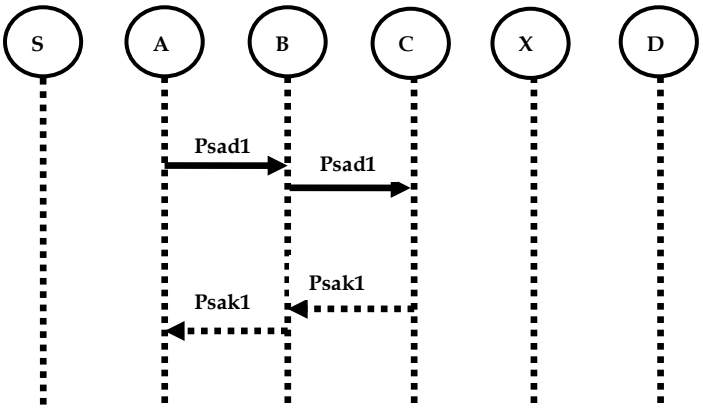

Fig.8. S-ACK Mode

4.3 MRA Mode

The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. The source node starts a AODV routing request to find another route. By adopting an alternative route to the destination node, we escape the misbehavior reporter node. Whenever the destination node receives an MRA packet, it searches its local storage and compares whether the reported packet was received or not. If it is already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious node otherwise the misbehavior report is trusted and accepted.

4.4 Hybrid Cryptographic Technique

This is an acknowledgement-based IDS. All three parts of the system, namely, ACK, S-ACK, and MRA, are acknowledgement based intrusion detection system. They all rely the acknowledgement packets to detect misbehavior's in the network. This is very important to ensure that all acknowledgement packets in the system are authentic. Otherwise, if the attackers are smart enough to forge acknowledgement data packets, all of the previous schemes will be vulnerable. With regard to this urgent concern incorporated Hybrid Cryptographic Technique in our proposed system. In order to ensure the integrity of the IDS, It requires all acknowledgement packets to be digitally signed before they are sent out and verified until they are accepted.

4.4.1 Formation of secret ACK data

The acknowledgement data can be encrypted with secret key of AES algorithm and generate secret data. The random number generator generate the random number and that number and the private key of RSA algorithm generate the digital sign. The ASCII value of secret data produce secret ACK data with the help of digital sign.

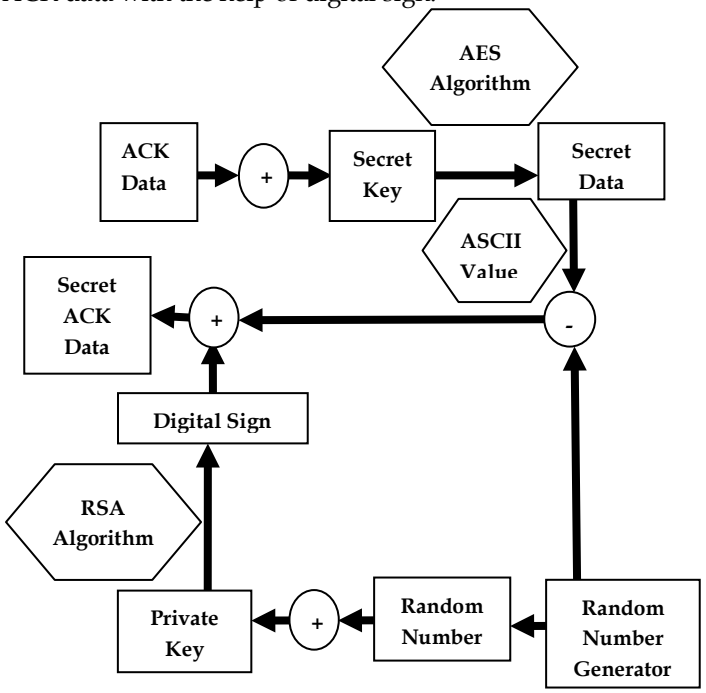

Fig.9. Formation of Secret ACK data

Algorithm

If data received

a. Checks I'm the destination
   i. If yes
      1. Generate the ack
         a. Set current time as ack time *Ta*
         b. Checks the pair-wise key b/w source and destination
            i. If found set key as $K_{S_{s-d}}$
         c. Split Ta into separate character $\cup T_{sA}$
         d. Create empty list for encrypted data El
         e. For-each char $Pt \in T_{sA}$
            i. Encrypt by AES algorithm
               1. $Pt => Ct$
               2. Convert to ascii value *Cta*
               3. *Generate random number(rand)*
               4. New value $Nv = Cta - rand$
               5. $(Cta \,\&\, Nv \& rand) \cup El$
            ii. Make digital sign
               1. *Checks for own private key*
               2. *For_each value of El*
                  a. Extract *Nv*
                  b. Encrypt by RSA private key
                     i. *Nv==>CNv*
                     ii. *CNv U Digital_sgn_lst*
      2. Send the secrete ack with
         a. Digital sign
         b. Rand number
         c. Generation time.

4.4.2 Verification of Acknowledgement

The randomized ASCII value generated from secret ACK data. Public key of RSA algorithm helps to verify the digital sign. It gives the verified ASCII char which generate secret message. That secret message with secret key of AES gives the ACK data.

Algorithm

If digital sign received in source

a. Node checks the public key info for ack generator
   i. If found
      1. decrypt by Pu ===>Ptrsa
      2. Checks for secrete pair key
         a. If found
            i. Decrypt Ptrsa by $K_{S_{s-d}}$ ==>*Pt*
      3. Pt U plain text list

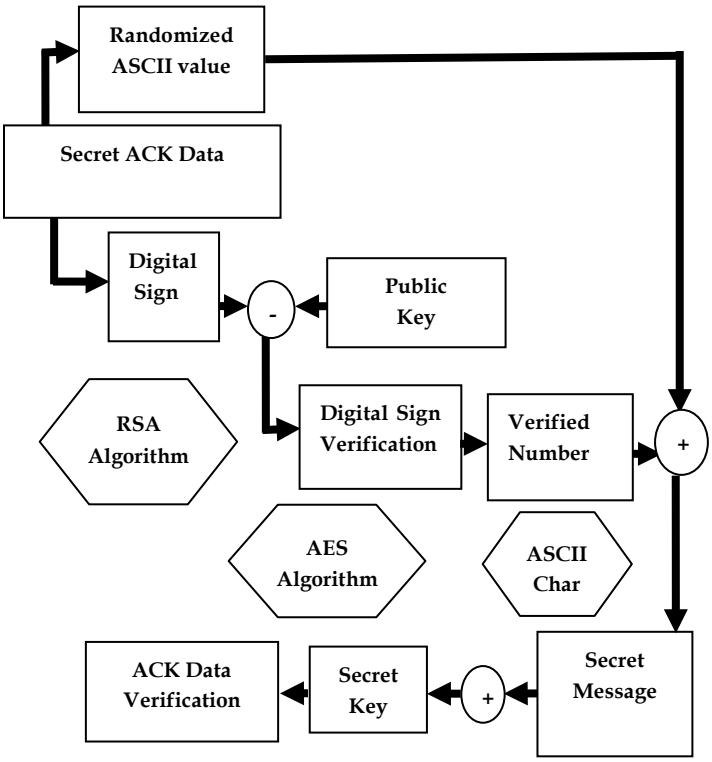

Fig. 10. Verification process of Secret ACK data

5 Simulation

5.1 Methodology

To better investigate the performance of Enhanced Intrusion Detection System with On-Demand Routing Protocol using Hybrid Cryptographic Techniques for MANETs under different types of attacks, we define three scenario settings to simulate different types of misbehaviors or attacks.

5.1.1 Scenario 1

In this scenario, we simulated a basic packet dropping attack from the malicious node. The malicious nodes simply drop all the packets that they receive. Purpose of this scenario is to test the performance of intrusion detection system against limited transmission power and receiver collision.

5.1.2 Scenario 2

This scenario is designed to test IDSs' performances against false misbehavior report generated by the node. In this situation, malicious nodes always drop the packets that they receive and send back a false misbehavior report whenever it is possible.

5.1.3 Scenario 3

This scenario is used to test the performances when the attackers are smart enough to forge acknowledgement packets and claiming positive result.

5.2 Configuration

The simulation is conducted within the Network Simulator(NS) 2.34 environment on a platform with GCC 4.3 and Ubuntu 10.04.4. The system is running on a laptop with

Core i7 CPU and 8-GB RAM. In order to better compare the simulation results with other research works, I adopted the default scenario settings in NS 2.34. The intention is to provide more general results and make it easier to compare the results. In NS 2.34, the default configuration specifies 10 nodes in a flat space with a size of 670 × 670 m. Both the physical layer and the 802.11 MAC layer are included in the wireless extension of NS2. The moving speed of mobile node is limited to 20 m/s and a pause time of 1000 s. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512 B. For each scheme, every network scenario three times and calculated the average performance.

6 Performance Evaluation

In To measure the performances of proposed scheme, we continue to adopt the following two performance metrics.

6.1 Packet delivery ratio(PDR)

PDR is the ratio between the total number of packet received at the destination node to the total number of packets sent by the source node.

6.2 Routing overhead (RO)

This is the ratio of routing related packets in bytes (RREQ, RREP, RERR, AACK,) to the total routing and data transmissions (sent or forwarded packets) in bytes. That means the acknowledgements and switching over head is included.

7 Simulation Results

In this section, the concentration goes on comparing performances through simulation result comparison with Watchdog, TWOACK, EAACK and Hybrid schemes.

7.1 Simulation Result- Scenario 1

In scenario 1, malicious nodes drop all the packets that pass through it. Fig. 11., shows the simulation results that are based on PDR. Proposed scheme Enhanced Intrusion Detection System with On-Demand Routing Protocol using Hybrid Cryptographic Technique for MANETs surpassed Watchdog's performance. From the results, the acknowledgement-based schemes, including TWOACK, AACK, EAACK and Hybrid scheme are able to detect misbehavior with the presence of limited transmission power and receiver collision. However, when the number of malicious nodes reaches 40%, proposed system performance is lower than those of TWOACK and AACK. It as a result of the introduction of MRA mode, when it takes more time to receive an MRA acknowledgement from the destination node that the waiting time exceeds the predefined threshold.

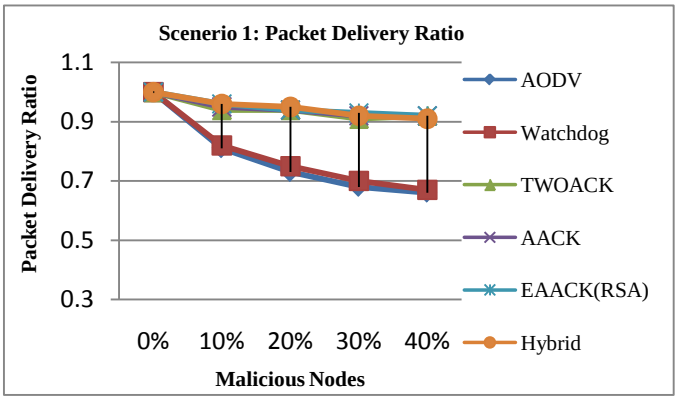

Fig.11. Simulation Result- Scenario 1- Packet Delivery Ratio

TABLE 1
SIMULATION DATA- SCENARIO 1

Scenario 1: Packet Delivery Ratio(PDR)					
Scheme	Malicious Nodes in %				
	0	10	20	30	40
AODV	1	0.81	0.73	0.68	0.66
Watchdog	1	0.82	0.75	0.7	0.67
TWOACK	1	0.94	0.94	0.91	0.92
AACK	1	0.95	0.94	0.92	0.92
EAACK(RSA)	1	0.96	0.94	0.93	0.92
Hybrid	1	0.96	0.95	0.92	0.91
Scenario 1: Routing Overhead(RO)					
Scheme	Malicious Nodes in %				
	0	10	20	30	40
AODV	0.02	0.23	0.73	0.68	0.66
Watchdog	0.02	0.025	0.025	0.025	0.025
TWOACK	0.19	0.4	0.43	0.44	0.53
AACK	0.19	0.23	0.3	0.34	0.39
EAACK(RSA)	0.16	0.31	0.38	0.46	0.56
Hybrid	0.15	0.28	0.37	0.46	0.56

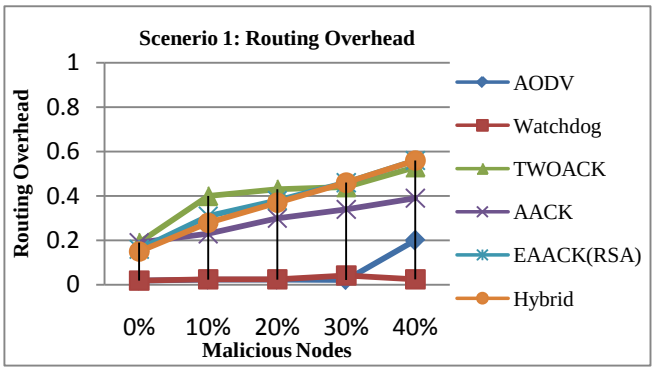

Fig.12. Simulation Result- Scenario 1- Routing Overhead

The simulation results of RO in scenario 1 are shown in Fig.

12. The AODV and Watchdog scheme achieve the best performance, because they do not require acknowledgement scheme to detect misbehavior activity. For the rest of the intrusion detection system, AACK has the lowest overhead.

7.2 Simulation Result- Scenario 2

In the second scenario, we set all malicious nodes to send out false misbehavior report to the source node whenever it is possible. Here, this scenario setting is designed to test the performance of intrusion detection system under the false misbehavior report. When malicious nodes are 10%, the proposed system performs better than AACK and TWOACK and same as EAACK. When the malicious nodes are at 20% and 30%, Hybrid scheme performs very good.

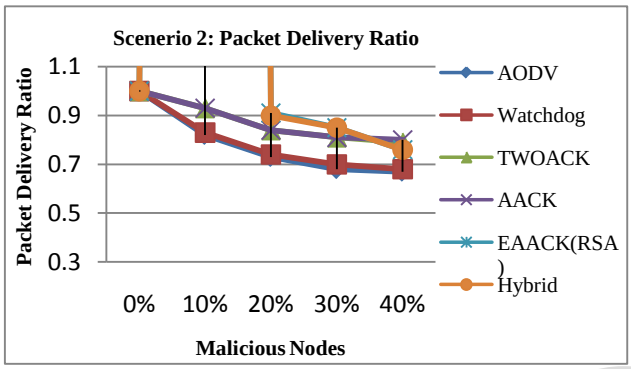

Fig.13. Simulation Result- Scenario 2- Packet Delivery Ratio

TABLE 2
SIMULATION DATA- SCENARIO 2

Scenario 2: Packet Delivery Ratio(PDR)					
Scheme	Malicious Nodes in %				
	0	10	20	30	40
AODV	1	0.82	0.73	0.68	0.67
Watchdog	1	0.83	0.74	0.7	0.68
TWOACK	1	0.93	0.84	0.81	0.79
AACK	1	0.93	0.84	0.81	0.8
EAACK(RSA)	1	0.94	0.91	0.85	0.76
Hybrid	1	0.94	0.9	0.85	0.76
Scenario 2: Routing Overhead(RO)					
Scheme	Malicious Nodes in %				
	0	10	20	30	40
AODV	0.02	0.023	0.023	0.022	0.02
Watchdog	0.02	0.025	0.025	0.023	0.023
TWOACK	0.18	0.2	0.37	0.41	0.4
AACK	0.18	0.2	0.23	0.22	0.52
EAACK(RSA)	0.23	0.26	0.34	0.36	0.69
Hybrid	0.22	0.25	0.31	0.24	0.66

In terms of RO, owing to the hybrid scheme, proposed system maintains a lower network overhead compared to TWOACK in most cases, as shown in Figure 14. However, RO rises rapidly with the increase of malicious nodes. It is due to the fact that more malicious nodes require a lot more acknowledgement packets and digital sign.

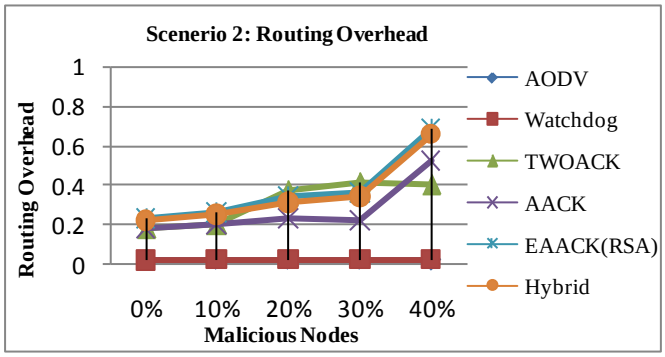

Fig.14. Simulation Result- Scenario 2- Packet Delivery Ratio

7.3 Simulation Result- Scenario 3

In scenario 3, have to provide the ability to forge acknowledgement packets to the malicious nodes. This way, the malicious nodes drop all the packets that they receive and send back forged positive acknowledgement packets to its previous node if necessary. Here, this is a common method for attackers to degrade network performance while still maintaining its reputation. Performance comparison of PDR in scenario 3 is shown in Figure 15. Proposed scheme outperforms TWOACK , AACK and EAACK in all test scenarios.

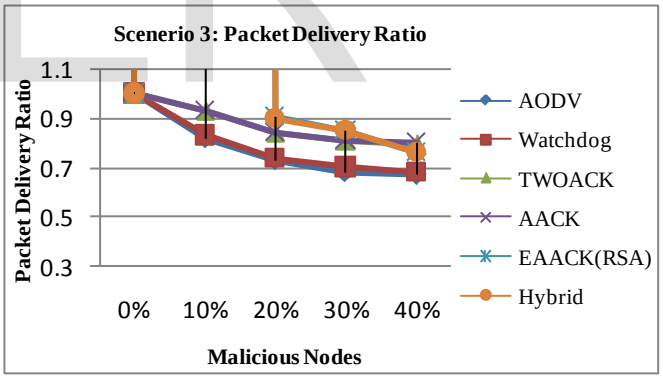

Fig.15. Simulation Result- Scenario 3- Packet Delivery Ratio

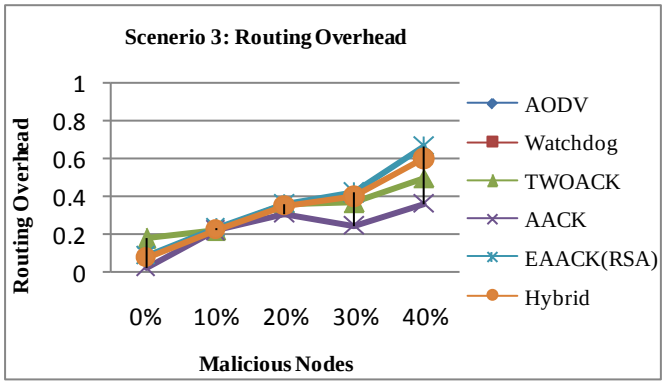

Figure 16 Simulation Result- Scenario 3- Packet Delivery Ratio

TABLE 3
SIMULATION DATA- SCENARIO 3

Scenario 2: Packet Delivery Ratio(PDR)					
Scheme	Malicious Nodes in %				
	0	10	20	30	40
AODV	1				
Watchdog	1				
TWOACK	1	0.92	0.78	0.67	0.61
AACK	1	0.92	0.78	0.66	0.61
EAACK(RSA)	1	0.93	0.82	0.77	0.76
Hybrid	1	0.93	0.82	0.77	0.76
Scenario 2: Routing Overhead(RO)					
Scheme	Malicious Nodes in %				
	0	10	20	30	40
AODV					
Watchdog					
TWOACK	0.18	0.22	0.36	0.37	0.5
AACK	0.03	0.22	0.31	0.25	0.36
EAACK(RSA)	0.09	0.24	0.36	0.42	0.67
Hybrid	0.08	0.23	0.35	0.4	0.6

Figure 16, shows the achieved RO performance results for each IDS in scenario 3. Hybrid scheme it produces more network overhead than AACK and TWOACK when malicious nodes are more than 10%. The reason is that hybrid scheme brings in more overhead than the other schemes.

8 CONCLUSION & FUTURE WORK

Packet dropping attack has always been a major threat to the security in mobile ad-hoc networks. In this research, we have proposed and implemented a Intrusion Detection System named Enhanced Intrusion Detection System with On-Demand Routing Protocol using Hybrid Cryptographic Technique for MANETs and compared it against other popular mechanisms in different scenarios. The results show positive performances against Watchdog, TWOACK, AACK and EAACK in the cases of different problems like limited transmission power, receiver collision and false misbehavior report. Consequential, in an endeavor to prevent the attackers from initiating forged acknowledgement attacks, We used hybrid cryptographic technique. It can improve the network's PDR when the attackers are smart enough to forge acknowledgement packets.

Eventually, we concluded that the Enhanced Intrusion Detection System with On-Demand Routing Protocol using Hybrid Cryptographic Technique for MANETs is more suitable to be implemented in MANETs. To increase the value of the project work, we plan to investigate the following issues in future work:

Testing the performance of this system in real network environment instead of software simulation.

1. Testing the performance of this system in real network environment instead of software simulation.

2. Possible to adopt other hybrid cryptographic methods instead of this hybrid technique.

REFERENCES

[1] EAACK—A Secure Intrusion-Detection System for MANETs, Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE

[2] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer- Verlag, 2008.

[3] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[4] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.

[5] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," IEEE Trans. Ind. Electron.,vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[6] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[7] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

[8] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[9] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 7, pp. 2759–2766, Jul. 2008.

[10] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl., 2002, pp. 3 13.

[11] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.

[12] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[13] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[14] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5,pp. 536–550, May 2007.

[15] K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile ad-hoc communications in AEC industry," J. Inf. Technol. Const., vol. 9, pp. 313–323, 2004.

[16] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 4,

pp. 1835–1841, Apr. 2008.

[17] Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC, 1996, T-37

[18] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.

[19] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[20] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE Int. Conf. Perform., Comput., Commun., 2004, pp. 747–752.

[21] Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless Conf., 2003, pp. 75–78.

[22] Perkins and E. Royer, "Ad-hoc on-demand Distance Vector Routing," Proc. 2nd IEEE Wksp. Mobile Comp. Sys. App., Feb. 1999, pp. 90–100.

[23] Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure routing and intrusion detection in ad hoc networks," in Proc. 3rd Int. Conf. Pervasive Comput. Commun., 2005, pp. 191–199.

[24] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1983.

[25] J. G. Rocha, L. M. Goncalves, P. F. Rocha, M. P. Silva, and S. Lanceros- Mendez, "Energy harvesting from piezoelectric materials fully integrated in footwear," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 813–819, Mar. 2010.

[26] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.

[27] Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in Communications in Computer and Information Science, vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387.

[28] Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[29] K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc networks on the mobile value system," in Proc. 2nd Conf. m-Bus., Vienna, Austria, Jun. 2003.

[30] Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.

[31] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proc. ACM Workshop Wireless Secur., 2002, pp. 1–10.

[32] L. Zhou and Z. Haas, "Securing ad-hoc networks," IEEE Netw., vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.

[33] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[34] TIK WSN Research Group, The Sensor Network Museum—Tmote Sky. [Online]. Available: http://www.snm.ethz.ch/Projects/TmoteSky.

[35] Y. Kim, "Remote sensing and control of an irrigation system using a distributed wireless sensor network," IEEE Trans. Instrum.Meas., vol. 57, no. 7, pp. 1379–1387, Jul. 2008.

AUTHOR PROFILE

Avinab Marahatta received Bachelor of Engineering in Computer Engineering from Purbancal University. He is pursuing Master of Technology in Computer Science. He worked in Higher Secondary Education Board(HSEB) Nepal, under the ministry of Education as Computer Engineer. His research interest are Computer Architecture, Human Computer Interaction, Wireless Network, Network Security and Data mining.

Kare Suresh Babu has completed his Master of Technology in Computer Science from Hyderabad Central University(HCU), Hyderabad.. He is the Asst. Professor and course coordinator for School of IT, JNTUH. His subjects of interests are Computer Networks, Network Security, Operating Systems, Wireless Networks, mobile Computing, Ethical Hacking and Wireless & Web Security.