Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 70 (2015) 341 – 347

Procedia
Computer Science

4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS 2015

# Analysis of Secure Routing Protocol for Wireless Adhoc Networks using Efficient DNA based Cryptographic Mechanism.

E.Suresh Babu[a,*] , C Nagaraju[b],MHM Krishna Prasad[c]

*Research Scholar , Dept of CSE, JNTUK, AP, India., sureshbabu.erukala@gmail.com*
*Associate Professor, Dept of CSE, YV University, AP, India.*
*Associate Professor, Dept of CSE, UEC,JNT University, AP, India.*

**Abstract**

This paper presents a novel concept for designing an efficient security solution that can protect wireless ad hoc networks from heterogeneous attacks. This proposed Secure Routing Protocol against Heterogeneous Attacks (SRPAHA) protocol effectively detects and defends the collaborative malicious node without the need of expensive signatures. Finally, this methods had been validated through numerous simulation scenarios that synthetically generates the data sets and verifies using various parameters such as Route Acquisition Time, Throughput (or packet delivery ratio), Routing Overhead and Average End-to-End Delay.Moreover, the results of this work provide better performances as compared to existing security schemes in-terms of security, less communication overhead.

*Keywords:* Heterogeneous Attack, Adhoc Networks.

## 1. Introduction

In today's computing world, with the advancement of wireless technology, mobile communication[2] has found its way to improve the living standard of our daily life. The rapidly growing of these technologies permits the users to access the information and service at anytime and anywhere, in spite of their geographic location. These advantages paved the way to resolve the issues such as efficiency, ease to use, and high deployment cost over conventional

* Corresponding author. E.SureshBabuTel.: +91-9440 959713 ;
*E-mail address:*sureshbabu.erukala@gmail.com

doi:10.1016/j.procs.2015.10.029

wired networks. Due to the diversity of applications, there is a necessity and growing interest of future wireless networks that need to be formed very quickly, almost spontaneously, decentralized Infrastructure, and dynamic network architecture that has led to the development of wireless ad hoc networks. The ad hoc networks are suitable, where existing fixed infrastructure is too expensive or inconvenient to employ for applications especially that are needed by governments, Law enforcement, Emergency scenarios, Military services, Commercial and Civil Applications and vehicular communications etc. Many wireless adhoc network applications require various routing protocols that need to operate properly even in hostile environments. As exchanging information between the mobile nodes over unprotected wireless links which are particularly vulnerable to different attacks[3,15]. Already a lot of work has been carried out on these networks to defend several existing routing protocols using conventional symmetric and asymmetric cryptographic mechanisms such as DES, RSA, ECC, etc. However, these mechanisms achieved very high level of security. Nevertheless, require complex factorization of large prime numbers[4,5] and addressing of the elliptic curve problem. A lot of investigation is still required to find a proper solution for these issues. The deployment of security in these routing protocols of wireless adhoc networks is still in their infancy with many security problems that are unsolved. Hence, security becomes a critical issue and poses new challenges for designing specialized security solutions of these networks. This paper presents efficient, lightweight cryptographic algorithms to design and analyse the secure routing protocols for providing the security solutions for specialized wireless ad hoc networks requiring less communication bandwidth and less memory in comparison with other cryptographic systems.The outline for the remainder of the paper is as follows. In Section-2 specifies the related work. Section-3built a heterogeneous attack model against adhoc routing protocols. Section-4 specifies DNA Based Hybrid Cryptographic Mechanism. In Section-5 addresses heterogeneous attack detection. Section-6specifies the simulation results. Finally, we discuss the conclusion with future work in Section-7

## 2. Related Work

Some of the researchers has already focused on a wide variety of black hole and wormhole attack detection, defending and avoiding techniques has been proposed in the literature. This section review some of the security attack, which is detrimental against both pro-active and reactive routing protocols.

In[6], Wang et al. proposed a end-to-end detection mechanism that categorizes wormhole attacks. This generic mechanism does not rely on neighbor trust, but it relies on end-to-end detection mechanism based on Cell-based Open Tunnel Avoidance (COTA). However, this mechanism requires a high storage power and computation, because wormhole detection packets are transmitted and the responses are used to compute each node's position and velocity. In[7], Tsou et al. introduced a reverse tracing technique to detect and prevent the black hole nodes against DSR routing protocol. In[8] Cheung et al. proposed multiple attacks model and developed a method based on typical isolated alerts about attack steps. In[9]Yang et al. proposed a signature-based mechanism to detect the collaborative attacks. Their technique is based on blind detection techniques, annotated topology information and multicasting. Shurmanet. al.[10] proposed two different techniques to detect the black hole attack against MANETS. However, their solution cannot handle to detect multiple black hole attack. In[11] Yu-Sung et al. proposed a collaborative IDS for different sorts of IDSs to work cooperatively. In[12] Hussain et al. proposed a collaborative system to detect distributed DoS (DDoS) attacks.

Most of the solutions discussed above are used to detect or avoid either black hole attacks or wormhole attack on routing protocols of mobile ad hoc networks. In this paper, a novel method is presented based on the AODV protocol in which the collaborative nodes are detected based upon the close neighborhood of the range and send the data packet with alternate path between source and destination. In addition, this work also defends the heterogeneous attack using SRPAHA mechanisms.

## 3. **Modelling a Heterogeneous Attack against Adhoc Routing Protocols:**

This section mainly addresses the Heterogeneous Attack, which may cause more devastating impacts on adhoc networks than single and uncoordinated attacks. In general, the heterogeneous attack model was developed to investigate the weaknesses of the routing protocols of mobile ad hoc network that exploits the vulnerabilities of adhoc environments, which will harm the system and results in a vulnerability assessment. This Heterogeneous

Attack makes use of the combined efforts of more than one attacker against the target victim. Moreover, this attack may launch multiple intruders to synchronize their activities and accomplish the usurpation, deception, disruption destruction, modification of data, and disclosure against targeted routing protocols to deny the services to legitimate nodes and completely terminate all activity to the network entities.

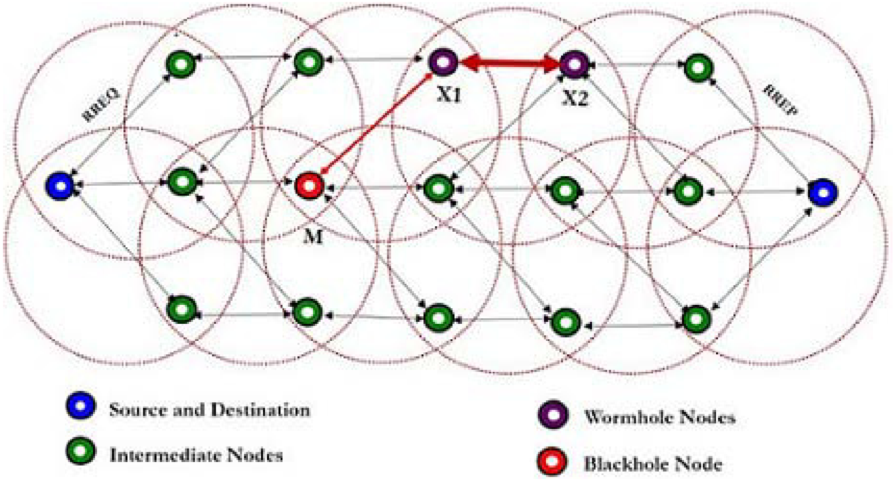

Fig-1: Illustrates the heterogeneous attack

Let us illustrate with an example, how the different attack takes place simultaneously to form heterogeneous attack. As shown from the following fig-1 We assume that the source node‘s’ sends the RREQ message to the destination node ‘d’ via some intermediate nodes. We assume that the one of the intermediate node ‘M’ perpetrates a black hole attack. Similarly, the intermediate nodes ‘X1’ and ‘ X2’ collude each other to carry out as wormhole attack. Here both M and ‘X1’ is compromised during the route discovery phase and collaborate each other. For instance, the malicious node ‘M’ could not tamper the RREQ message that was received from the source, and simply replies with a RREP packet stating that has the shortest path to destination node ‘D’. Then the malicious node ‘M’ will establish a route through the intermediate node ‘X1’ which in turn forward the packets to another node ‘‘ X2’ with the help of the tunnel and retransmits them there into the network. After the route discovery setup, the malicious node ‘M’ could not tamper or drop the message that was received from source, but, may forward the message to ‘X1’ node, then the malicious node ‘X1’ and ‘X2’ receives every packet from the blackhole node ‘M’ and they can tamper the contents or simply drop them selectively. This specific example illustrates that such a heterogeneous attack is more devastating on adhoc networks.

## 4. Secure Routing Discovery Mechanism using DNA based Cryptography

In the layer-5 of the OSI network model, most of the possible attacks will be either on routing information or data tampering. The prevention of these attacks against on-demand routing protocols can be performed using authentication and encryption mechanism.

### *4.1 Overview of AODV Routing Protocol:*

In brief, to summarize the AODV[13] routing protocol. AODV is the predominant on-demand routing protocol that offers low processing, low network utilization, ability to adapt the dynamic conditions and low memory overhead. We used this AODV as an underlying protocol to protect from the heterogeneous attack. The functionality of AODV is usually initiated with the route discovery process, whenever a valid route is not present, and another mechanism is route maintenance, as AODV fails to maintain lifelong route between the sending node and receiving node, due to the high mobility by nature. This proposed work modifies the original AODV protocol[14]. The slight modification is done at the destination side. To be more specific, the destination node broadcast the Route Reply (RREP) packet back to all its neighbor nodes with the current route until reaches to the source node to create multiple route, instead of unicasting as in the original AODV routing protocol. To adapt the dynamic topology environment in the route discovery process of AODV in ad hoc networks, we used multiple, possibly disjoint, routes/path between source and destination. The alternative multiple paths between source and destination can be used for two purpose, first if the primary path fails to send the packets to the destination. Second, after detection of heterogeneous attack, source node will diverted the traffic with alternate route to the destination. Finally, once the path is entrenched, the nearest neighbor nodes will monitor the link status for the active routes. The nodes that do not conformed the neighbor rating based on neighbor profile will be eliminated from the route

### *4.2 Modelling a DNA Assembled Public Key (DAPK) Cryptography*

A DNA assembled public key encryption scheme[17] makes use of asymmetric encryption scheme (We used underlying RSA Algorithm for encrypting the plain text message, which is one of the *public key cryptosystem.*)for effective storage of cipher text and public key in the DNA strand. Moreover, this method, first, it provides double encryption, which is very difficult for adversary to break the cryptosystem. Second, it provides more compact storage space, which is more suitable for public key encryption. In our case, RSA public keys require huge storage for storing large prime numbers. While DNA assembled public key cryptography, take less storage than public encryption algorithm

### *4.3 Modelling a Pseudo DNA based Symmetric Cryptosystem:*

In[1], we proposed a novel method called pseudo symmetric DNA based cryptographic mechanisms. This pseudo DNA based symmetric cryptography mechanism is mainly used to achieve data integrity and confidentiality.

### *4.4 Node Authentication using Hybrid DNA based Cryptosystem:*

This section describes the hybrid DNA based cryptosystem, which is used to verify the data integrity and authenticate the mobile nodes. Moreover, this hybrid approach makes use of both the public and private key-based schemes. Here, symmetric encryption will be used to achieve integrity and confidentiality, while asymmetric encryption will provide to authenticate the members of mobile nodes. In order to authenticate the mobile nodes and to establish the session keys, the following framework is used.

- Initially, a node ‘S’ generates a pair of DNA secret key K(PR,S) and public key K(PU,S) and distributed the public key K(PU,S) to the node ‘D’ by using Public Key Infrastructure or Trusted Authority.
- Similarly, a node ‘D’ also generates a pair of DNA private key K(PR,D) and public key K(PU,D) and distributed the DNA public key K(PU,D) to the node ‘S’ by using PKI or CA.
- If the node ‘S’ and node ‘D’ are 1-hop neighbors then Node ‘S’ can authenticate the node ‘D’ by issuing a signed certificate with its DNA private key. Here certificate is a proof of node ‘D’ ID and DNA public key with ‘S’ signature.
- If any of the intermediate nodes ‘w' want the read the signed certificate, he/she should hold ‘S’ DNA public key and then node ‘w’ can read and trust that node by bind it along its DNA public key.
- Finally, N-hop one to one intermediate nodes can quickly create a DNA private key by using three-way handshake based on the key information and availability of certificates in the PKI[16].

## 5. Heterogeneous Attack Detection:

This sub-section performs the next task, after developing the secure route discovery process on the AODV routing protocol, the detection scheme against heterogeneous attack,which is incorporated into secure route discovery procedures.To detect the cooperative misbehaving nodes, first, the all nearest neighbour and foreign neighbour nodes profile approach[18] are used. In this approach, each node finds its closest nearest neighbour and foreign neighbour between the sender and receiver via neighbour nodes. To be more specific, Let $n_1$ be the nearest node to M ,$n_2$ be nearest neighbor node to $X_1$ and foreign neighbor to $n_1$ and $n_3$ be nearest neighbor node to $X_2$and it is nearest foreign neighbor to $n_2$ and so on. Subsequently, all the nearest neighbour and foreign neighbour$n_1$, $n_2$,$n_3$

between the sender ‘s’ and receiver ‘d’ will estimate the malicious nodes antiquity by neighbour rating of $M$, $X_1$ and$X_2$ respectively. All the neighbor node will share the unique DNA based secret shared key between the sender and neighbour nodes.The node $n_i$ is the neighbor to M but cannot reach to $\mathrm{X}_1$ , node $n_j$ is the neighbor to $\mathrm{X}_1$ completely know the profile of $\mathrm{X}_1$ but cannot reach to $\mathrm{X}_2$ and node $n_k$ is the neighbor to $\mathrm{X}_2$ completely know the profile of $\mathrm{X}_2$ . since$n_k$ is already neighbor to $n_j$ , and $n_j$is already neighbor to $n_i$. who completely gives opinion of M, $\mathrm{X}_1$and $\mathrm{X}_2$to the source node. Subsequently, In a future behavior between M, $\mathrm{X}_1$and $\mathrm{X}_2$ will be monitored by $n_i$ , $n_j andn_k$, the probability of this nodes behavior will be rated by both the nodes $n_i, n_j andn_k$is:

$$LetD_{X1,\mathrm{X2}} = alltheencounters(neighborrating)betweenX_1andX_2ismonitoredbyn_k$$

$$X_{X1,\mathrm{X2}}(y) = \ indicatorvariablefornoden_kfortheconfirmationofmaliciousnodeX_2atencountery$$

$$P(X_{j,X2}(y+1)=1) \mid D_{j,k}\ , D_{k,X2}$$

$$= P(X_{j,k}(y+1)=1)|D_{j,k}\ \cdot, P(X_{k,X2}(y+1)1)|D_{k,X2}+$$

$$[1 - P(X_{j,k}(y+1)=1)\ \mid D_{j,k}] \cdot [1 - P(X_{k,X2}(y+1)=1) \mid\ D_{k,X2}]$$

$$= \ r_{j,k}r_{k,X2} + \ (1 - r_{j,k}) \cdot (1 - r_{k,X2}) \qquad (1)$$

$$LetD_{M,\mathrm{X1}} = alltheencounters(neighborrating)between\ \ \mathrm{M}\ andX_1is$$

$$monitoredbyn_iandn_j$$

$$X_{M,\mathrm{X1}}(y) = \ indicatorvariablefornoden_jfortheconfirmationofmaliciousnodeX_1atencountery$$

$$P(X_{i,X1}(y+1)=1) \mid D_{i,j}\ , D_{j,X1}$$

$$= P(X_{i,j}(y+1)=1)|D_{i,j}\ \cdot, P(X_{j,X1}(y+1)1)|D_{j,X1}+$$

$$[1 - P(X_{i,j}(y+1)=1)\ \mid D_{i,j}] \cdot [1 - P(X_{j,X1}(y+1)=1) \mid\ D_{j,X1}]$$

$$= \ r_{i,j}r_{j,X1} + \ (1 - r_{i,j}) \cdot (1 - r_{j,X1}) \qquad (2)$$

$$LetD_{s,m}(y)alltheencounters(neighborrating)betweenSand\ \mathrm{M}$$

$$ismonitoredbyn_i$$

$$X_{s,m}(y) = \ indicatorvariablefornoden_ifortheconfirmationofmaliciousnodeMatencountery$$

$$P(X_{s,m}(y+1)=1) \mid D_{s,i}\ , D_{i,m}$$

$$= P(X_{s,i}(y+1)=1)|D_{s,i}\ \cdot, P(X_{i,m}(y+1)=1)|D_{i,m}+$$

$$[1 - P(X_{s,i}(y+1) = \qquad 1)\ \mid D_{s,i}] \cdot [1 - P(X_{i,m}(y+1)1) \mid\ D_{i,m}]$$

$$= \ r_{s,i}r_{i,m} + \ (1 - r_{s,i}) \cdot (1 - r_{i,m})\ (3)$$

The interpretation of the equations 1st ,2nd and 3rdgives the probability of$n_i, n_j andn_k$, that agree and approves the nodes $\mathrm{M}\,,\mathrm{X}_1$ and $\mathrm{X}_2$ is misbehaving. Hence, the nearest neighbour and foreign neighbours can identify the misbehaving nodes by monitoring the network traffic of its neighbouring nodes. After detecting the collaborative malicious node based on both neighbour direct rating and foreign neighbour indirect rating, the source node will divert the traffic with different route to the destination. Eventually, the intrusion of collaborative malicious node effect to network becomes weaker. Once again, we can conclude that the more paths reduce collaborative malicious node intrusion to the network. In summary, the heterogeneous intrusion can be identified without the need of expensive signatures, as these signatures, which can be used to defend the route from end to end.

## 6. Simulation Results and Performance Analysis:

To study the feasibility of our theoretical work, we have implemented and evaluated the SRPAHA method using the network simulator [NS2], which is a software program running in Ubuntu-13.04 and conducted a series of experiments to evaluate its effectiveness. The experiment results show that this method is more efficient and increase the power against heterogeneous attacks. Our simulations are mainly used to compare between SRPAHA with AODV routing protocol with and without the presence of malicious nodesand ARAN respectively. To evaluate the SRPAHA, we considered various performance metrics such as Packet Delivery Ratio (PDR), Average End-to-End-Delay and routing overhead. As shown in fig-2 and fig-3, the packet delivery fraction of SRPAHA is higher in both the 30 and 50 node scenarios. Subsequently, nearly identical to AODV routing protocol at different speeds. However, AODV decreases in the presence of heterogeneous attack (one black hole node and one collaborative worm hole nodes), which delivers lesser data packets and routing packets to the destination. To be more specific, 7% of data packets are dropped, without delivering to the destination. While, SRPAHA, detects the heterogeneous attack with the help of IDSAHA and removed from the routing based on neighbour rating. Hence, SRPAHA using IDSAHA is extremely efficient in the route discovering, monitoring the routing process and maintaining multiple path for delivery of data packets in the presence of heterogeneous attack. Furthermore, it is also seen that SRPHDC always outperforms ARAN, as ARAN fails to handle the wormhole attack. While, SRPAHA effectively detects, defends the wormhole attack and delivers more data packets to the destination than ARAN. Hence, SRPAHA has a higher PDR than ARAN.

As shown in fig-4 and fig-5. End to End Delay of SRPAHA and AODV at different speeds. AODV reduces the PDR in high mobility (maximum speed increases from 1.5 and 10 milliseconds) conditions, because more link breakage between source and destination, Therefore, as maximum speed increases the PDR decreases. As compared toAODV, SRPAHA always has a lower End-to-End packet latency in high mobility conditions. Moreover, SRPAHA make use of multipath routing, if one path fails, an alternate path will immediately be available. However, IDSAHA incurs a delay while detecting the heterogeneous attack (HA).The figures also show the End-to-End packet latency

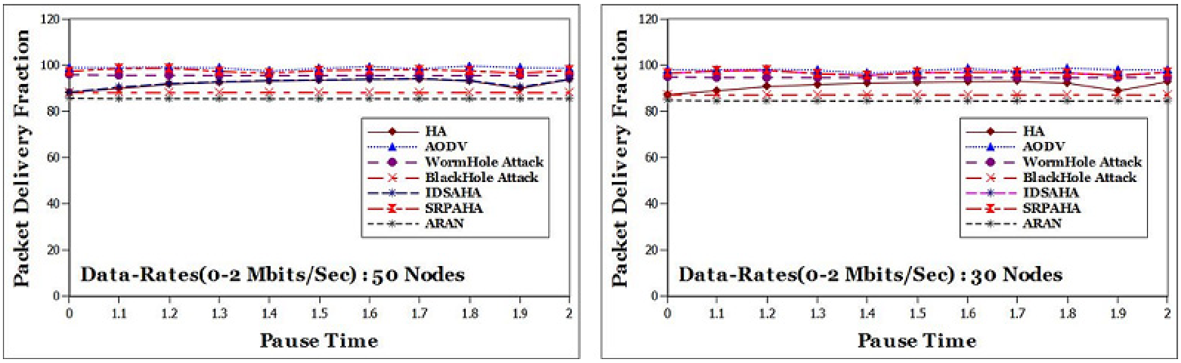

Fig-2 and Fig-3: Packet Delivery Ratio for 30 and 50 Nodes

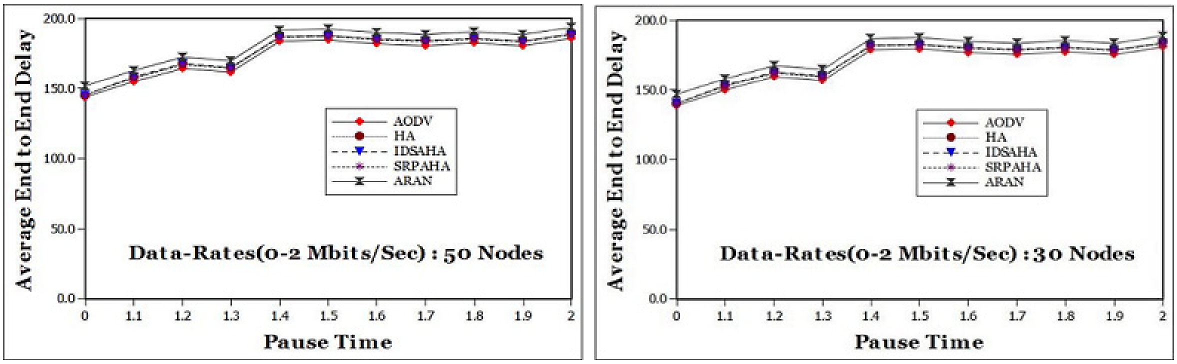

Fig-4 and Fig-5: Average End-to-End Delay for 30 and 50 Nodes

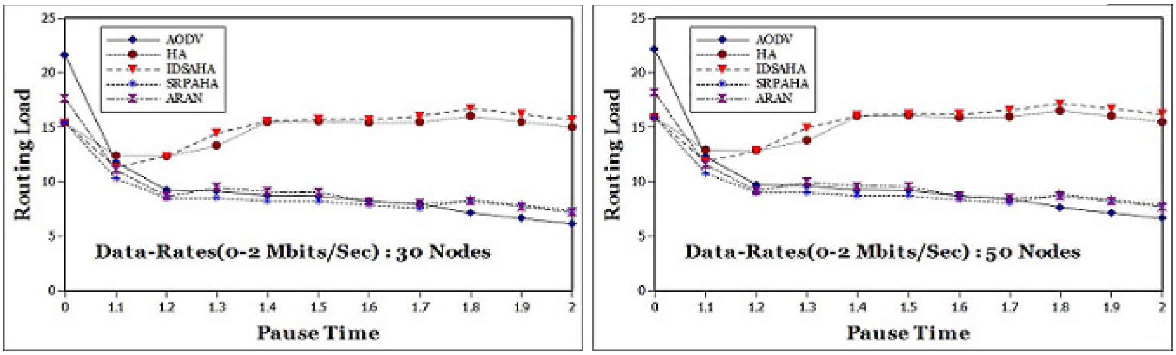

Fig-6 and Fig-7: Routing Load for 30 and 50 Nodes of SRPAHA and ARAN. In this case, it is observed that SRPAHA has lower latency than ARAN, Since, SRPDHC make use of parallel computation that causes less overhead of cryptographic operations than ARAN. In ARAN, while processing the control packets, each and every node has to verify the signature and replace with its own digital signature that cause more overhead using conventional cryptography and additional delays at each node. Therefore, the End-to-End packet latency increases.The fig-6 and fig-7 depicts the total overhead of SRPAHA in comparison with AODV Here, it is observed that SRPHDC gives slight overhead than AODV due to the security mechanism in the presence of different numbers of heterogeneous attack. Moreover, SRPAHA make use of IDSAHA that can detect the heterogeneous attack based on neighbour rating and remove them from the route. From the figure; it is also observed that SRPAHA gives less overhead than ARAN, because SRPHDC uses a light weighted cryptographic mechanism.

## 7. Conclusion and Discussion

This paper addressed a scheme for designing an efficient security solution that can protect wireless adhoc networks from heterogeneous attacks. Initially, we had modelled and investigated heterogeneous attack that exploits the vulnerabilities of the existing AODV routing protocols of wireless ad hoc network. Particularly, the proposed SRPAHA protocol establishes cryptographically secure communication among the nodes using Hybrid DNA-based Cryptography (HDC). HDC is one of the prospective methodology for sophisticated wireless adhoc network, which require less computational power, communication bandwidth and memory in comparison with other cryptographic systems. The simulation results of this work to provide better security, less computation overhead and network performances as compared to an existing ARAN scheme.

## References

1. Babu, E. Suresh, C. Naga Raju, and Munaga HM Krishna Prasad. "Inspired Pseudo Biotic DNA Based Cryptographic Mechanism Against Adaptive Cryptographic Attacks." Published in International Journal of Network Security, Vol.18, No.2, PP.291-303, Mar. 2016
2. Raychaudhuri and N. B. Mandayam, “Frontiers of Wireless and Mobile Communications,” Proc. IEEE, vol. 100, no. 4, pp. 824–840, Apr. 2012.
3. Wu, J. Chen, J. Wu, and M. Cardei, “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”, 2007.
4. Y. Brun, “Nondeterministic polynomial time factoring in the tile assembly model,” Theoritical Computer Science, Science Direct, Elsevier, vol. 395, no. 1, pp. 3–23, Apr. 2008.
5. D. Beaver, “Factoring: The DNA solution,” in 4th International Conferences on the Theory and Applications of Cryptology. Wollongong, Australia: Springer-Verlag, Nov. 1994, pp. 419–423.
6. W. Wang, B. Bhargava, Y. Lu, and X. Wu, “Defending against wormhole attacks in mobile ad hoc networks,” Wirel. Commun. Mob. Comput., vol. 6, no. 4, pp. 483–503, 2006.
7. P-C Tsou, C. J-M Chang, Y-H Lin, H-C Chao, J-L Chen, “Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs”, Feb. 13~16, Phoenix Park, Korea, 2011,
8. Cheung S, Lindqvist U, Fong M. Modeling multistep cyber attacks for scenario recognition. In DARPA Information Survivability Conference and Exposition, Vol. 1, 2003; 284–292.
9. Yang J, Ning P, Wang XS, et al. CARDS: A distributed system for detecting coordinated attacks. In Proc. of IFIP TC11 16th Annual Working Conference on Information Security, 2000.
10. Al-Shurman, M., Yoo, S. and Park, S., "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, pp. 96-97, 2004
11. Yu-Sung W, Foo B, Mei Y, Bagchi S. Collaborative intrusion detection system (CIDS): a framework for accurate and efficient IDS. In Proc. Computer Security Applications Conference (ACSAC '03), 2003.
12. Hussain A, Heidemann J, Papadopoulos C. COSSACK: coordinated suppression of simultaneous attacks. In DISCEX, 2003.
13. C. E. Perkins and E. M. Royer, “The ad hoc on-demand distance-vector protocol,” in Ad Hoc Networking, C. E. Perkins, Ed. Reading, MA: Addison-Wesley, 2001, ch. 6, pp. 173–220.
14. E. S. Babu, “An Implementation and Performance Evaluation Study of AODV, MAODV, RAODV in Mobile Ad hoc Networks,” vol. 4, no. 9, pp. 691–695, 2013.
15. E. S. Babu, C. Nagaraju, and M. H. M. K. Prasad, “An Implementation and Performance Evaluation of Passive DoS Attack on AODV Routing Protocol in Mobile Ad hoc Networks PROTOCOL OF,” vol. 2, no. 4, 2013.
16. S. Capkun, L. Buttyan, and J. Hubaux, “Self-organized public-key management for mobile ad hoc networks,” IEEE Trans. Mobile Comput., vol. 2, no. 1, pp. 1–13, Jan.–Mar. 2003.
17. Babua, E. Suresh, C. Nagarajub, and MHM Krishna Prasadc. "Light-Weighted DNA based Hybrid Cryptographic Mechanism against Chosen Cipher Text Attacks."published in International Journal of Information Processing, 9(2), 57-75, 2015,ISSN:0973-8215,IK International Publishing House Pvt. Ltd., New Delhi, India
18. AlexandrAndoni” Nearest Neighbor Search” in PhD Thesis, Massachusetts Institute Of Technology September 2009