International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 4 2356 – 2361

A Protective Mechanism to Avoid Eavesdropping Attack in MANET

Rajani B. Patil
Department of Computer Engineering
Dr. D.Y.Patil College of Engineering
Ambi, Pune,India
sunshinerajani@gmail.com

Prof. Dhanashree Kulkarni
Department of Computer Engineering
Dr. D.Y.Patil College of Engineering
Ambi, Pune,India
dskulkarni10@gmail.com

Abstract**—**Wireless ad hoc network is self-directed and infrastructure less network. Wireless ad hoc network is particularly inclined due to its basic characteristics, such as open medium, dynamic topology, distributed cooperation, and capability constraint. Routing plays an imperative part in the security of the whole system. Secure transmission of data in wireless ad hoc environment is an imperative concern. Any aggressor get remote flag by using transceiver and without being caught. The objective of this paper is to propose new secure unobservable routing protocol where attacker gets blocked while making spoofing or DOS attacks. Only oblivious message could be gathered by attacker. Proposed protocol will also protect privacy information among network and will detect and block attacking nodes through trust mechanism.

Keywords*-DOS attack; spoofing; dynamic topology; Routing; secure unobservable routing protocol*

*****

I. INTRODUCTION

A wireless adhoc network is collection of thousands of tiny wireless sensor nodes for data communication purpose. These sensor nodes coordinate with one another to fulfill information transmission. Numerous applications built in WSN are security, inventory tracking, automotive control, surveillance, health monitoring and other civil tasks, bridge monitoring, home automation in the recent years. Sensors are modest, low power gadgets, which have restricted assets.

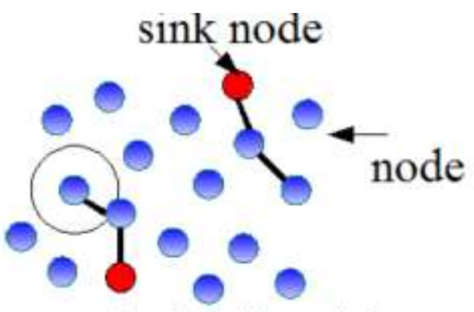

Fig ure 1: WSN Architecture

Fig.1 shows system architecture of wireless sensor network. The quantity of sensor hub in WSN are normally huge. Every node contains a power unit, a processing units, a storage units, sensing unit and wireless transmitter. The Sensor nodes intercommunicate with each other through simultaneous transmission of data from one node to another node. As range of transmitter is limited, data must be forwarded in multiple host in order to reach remote node which is at long distance from originating source node. Cost of sensor node is dependant on applications complexity.The sensors are still available at minimum cost. Most of the time, star topology is used in WSN.

A. Privacy Preserving Security Parameters in MANET

1. **Anonymity[1],[2]** is the state of being not identifiable within a set of subjects, the anonymity set i. e. Hiding source of data.
2. **Unlinkability[1],[2]** of two or more (Identity of Intrest)IOIs means these IOIs are no more or no less related from the attacker's view i. e. Hiding actual contents of data.
3. **Unobservability[1],[2]** of an IOI is the state that whether it exists or not is indistinguishable to all unrelated subjects, and subjects related to this IOI are anonymous to all other related subjects.

B. Problem Description

The main objective is to develop a new unobservable secure on demand routing protocol(USOR)[2] where attacker get blocked while making spoofing or DOS attacks. Following key objectives are also considered,

- ✓ To make Sender, intermediate and destination node not identifiable in network
- ✓ To protect Link Information
- ✓ To collect only unobserved message by attacker
- ✓ To protect nodes which get easily compromised by attacks by privacy preserving routing protocol.
- ✓ To discover and block assaulting nodes through trust mechanism.

C. Problem Identification

Numerous privacy-preserving routing schemes have been proposed. And the issues in current anonymous routing protocols are listed below:

1. Current anonymous routing protocols mainly consider anonymity and partial unlinkability in MANET.

2. Complete unlinkability and unobservability are not guaranteed due to partial content protection.

3. Present schemes encounters source traceback attacks as information like packet type and sequence number etc. can be used to relate two packets, which cracks unlinkability.

4. An insight on utilizing which key for unscrambling should be provided in each encoded packet, which demands careful design to eliminate linkability.

To provide strong privacy in MANET, unobervable secure on-demand routing protocol must provide Content Unobservability and Traffic Pattern Unobservability.

- ✓ *Content Unobservability[2]* : Adversary never obtain useful information from content of any message. It can be achieved by using novel combination of group signature and ID based encryption.

- ✓ *Traffic Pattern Unobservability[2]* : Adversary unable to achieve useful information from recurrence, length, and sender- receiver patterns of message traffic. It can be achieved by incorporating traffic padding.

II. Related Work

There are number of anonymous routing schemes available in ad hoc network which provide various levels of privacy protection at different cost. Most of them rely on public key cryptosystems (PKC) to attain anonymity and unlinkability in routing. Extensive computation overhead introduced due to expensive PKC operations.

The ANODR protocol proposed by Kong et al. [3] is the first to give anonymity and unlinkability for directing in ad hoc network. ANODR is using one-time public/private key pairs to achieve anonymity and unlinkability which is based on Onion Routing which is used for route discovery but design of ANODR unable to acheive unobservability. The PKC encryption/decryption and one-time public/private key pairs generation in ANODR increases the computation overhead for mobile nodes in ad hoc network.

One-time public/private key pairs are used by ASR [6], ARM [8], AnonDSR [9] and ARMR [10] to attain anonymity and unlinkability. The design of ASR[6] is made to achieve stronger privacy location that that of ANODR[3] as nodes on route are not having any information of their distance to the source/destination node. ARM[8] is used to reduce computation overhead on one-time public/private key pair generation.

Secure distributed anonymous routing (SDAR)[11] scheme proposed by A. Boukerche, K. El-Khatib, L. Xu, and L. Korba is working with long-term public/private key pairs at each node for anonymous communication. It is more scalable to network size and having large computation overhead.

On-demand anonymous routing (ODAR)[12] scheme proposed by D. Sy, R. Chen, and L. Bao yields only identity anonymity. It is not providing unlinkability for MANET, since the whole RREQ/RREP packets are not secured with session keys.

MASK[13] proposed by Y. Zhang, W. Liu, and W. Lou is anonymous on-demand rouitng protocol which achieve both MAC-layer and network-layer communications without disclosing real IDs of the participating nodes. It is based on the pairing-based cryptosystem, to attain anonymous communication in MANET. Here, trusted authority generate adequate pairs of secret points and related pseudonyms as well as cryptographic parameters. MASK scheme setup is expensive and RREQ flag is not secured and causes a passive adversary to identify the source node. Hence, adversary can recuperate linkability between different RREQ packets with the same destination, which violates receiver anonymity.

An anonymous location-aided routing scheme (ALARM)[5] proposed by K. E. Defrawy and G. Tsudik is using combination of public key cryptography and the group signature to conserve privacy. Privacy preserving feature is provided by group signature where everyone can verify a group signature but cannot get information of who is the signer. But ALARM outflows information like location of node and topology used in network.

To condense, public key cryptosystems have a best asymmetric feature, and it is appropriate for protection insurance in MANET. Most of anonymous routing schemes proposed for MANET are using public key cryptosystems to guard privacy. Only anonymity and unlinkability is provided by present schemes and unobservability is not yet considered and employed.

III. USOR Protocol

A. Modules

The process has been isolated into following three modules,

1) Key Generation
   - I. Group Signature Scheme.
   - II. ID-based Encryption Scheme.
2) Anonymous Key Establishment
3) Privacy-Preserving Route Discovery
   - I. Route Request.
   - II. Route Reply.
   - III. Attack Analysis.
   - IV. Data Transmission.

B. Key Generation[2]

In group signature scheme, each member of group is allowed to sign a message on behalf of the group. The key server produces a *group public key PUgp* which is publicly known by everyone. It generates a *private group signature key PRx* for each node X. ID-based encryption is a type of public-key encryption where the public key of a user is unique data about the identity of the user, which enabled users to validate digital signatures using only public information such as the user's identifier.

ISSN: 2321-8169
2356 – 2361

C. *Anonymous Key Establishment[2]*

Fig 2. Shows Anonymous Key Establishment with its neighbours. Fig 3. Shows flow chart for Anonymous Key Establishment. Here, each node in ad hoc network interact with its direct neighbours inside its radio extent for anonymous key establishment.

1. **S** → * : r_S P , SIG $_{gsks}$ (r_SP)
2. **X** → **S** : r_X P , SIG $_{gsks}$ (r_XP), E_{kSX} ($\bar{k}_{X*}$)
3. **S** → **X** : E_{kSX} ($\bar{k}_{S*}$)

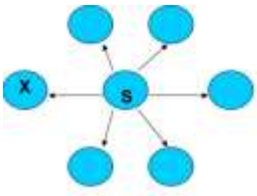

Figure 2: Anonymous Key Establishment

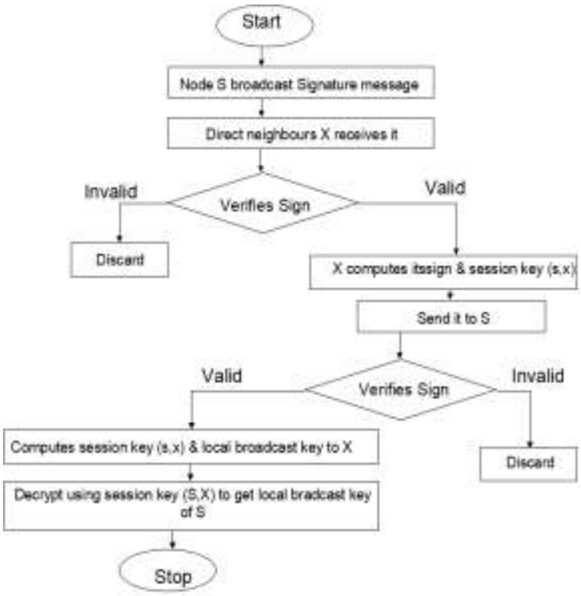

Figure 3: Anonymous Key Establishment Flowchart

D. *Route Request[2]*

S selects a random number r_S, and uses the identity of node D to encode a trapdoor information that only can be opened with D's private IDbased key, which yields ***ED(S,D, rSP)***. S then chooses a sequence number *seqno* for this route request, and another random number N_S as the route pseudonym, which is used as the index to a specific route entry.

Each node also maintains a temporary entry in his routing table

(seqno,Prev_RNym,Next_RNym,Prev_hop,Next_hop),

Where, *seqno* is the route request, sequence number,

Prev_RNym is the route pseudonym of previous hop,

Next_RNym is the route pseudonym of next hop,

Prev_hop is the upstream node

Next_hop is the downstream node along the route.

nonce is an arbitrary number used only once in a cryptographic communication.

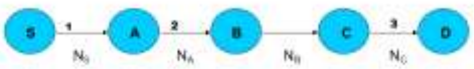

Figure 4: Route Request

(1): $Nonce_S$, Nym_S , $E_{K\text{-}S*}$(RREQ,N_S,E_D (D, S, r_SP),seqno)
(2): $Nonce_A$, Nym_A , $E_{K\text{-}A*}$(RREQ,N_A,E_D (D, S, r_SP),seqno)
(3): $Nonce_C$, Nym_C , $E_{K\text{-}C*}$(RREQ,N_C,E_D (D, S, r_SP),seqno)

E. *Route Reply[2]*

After node D realizes that he is the destination node, he starts to prepare a reply message to the source node. For route reply messages, unicast message is used to save communication cost.

D selects a random number r_D and generate a ciphertext ***ES(D, S, r_SP, r_DP)*** showing that he is the valid destination capable of opening the trapdoor information.

When C obtains the above message from D, he determines who is the sender of the message by evaluating the equation ***Nym_{CD} = H3(k_{CD}|$Nonce_D$)***. So he uses the correct key k_{CD} to decrypts the ciphertext, then he finds out route corresponding to RREP message according to the route pseudonym N_C and seqno. C then searches his route table and modifies the temporary entry ***(seqno,N_B,N_C,B,−)*** into ***(seqno,N_B,N_C,B,D)***.

At the end, C chooses a new nonce $Nonce_C$, computes

Nym_{BC} = H_3(k_{BC}|$Nonce_C$)

sends the following message to B:

($Nonce_C$, Nym_{BC}, E_{kBC} (RREP, N_B, E_S(D,S,r_SP,r_DP), seqno)

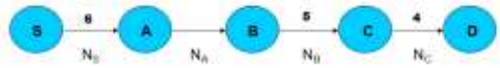

Figure 5: Route Reply

(4): $Nonce_D$, Nym_{CD} , E_{KCD}(RREP,N_C,E_S (D, S, r_SP,r_DP),seqno)
(5): $Nonce_C$, Nym_{BC} , E_{KBC}(RREP,N_B,E_S (D, S, r_SP,r_DP),seqno)
(6): $Nonce_A$, Nym_{SA} , E_{KSA}(RREP,N_S,E_S (D, S, r_SP,r_DP),seqno)

F. *Unobservable Data Transmission[2]*

After the source node S successfully searches a route to the destination node D, S can begin to send unobservable data transmission under the protection of pseudonyms and keys.

Node A comes to know that this message is for him according to the pseudonym Nym_{SA} after receiving the above message from S. After deciphering using the correct key, A identifies that this message is a data packet and should be forwarded to B by looking at value of route pseudonym N_S. Hence he prepares and forwards the following packet to B:

$Nonce_A$,Nym_{AB},E_{kAB}(DATA,N_A, seqno,E_{kSD}(payload))

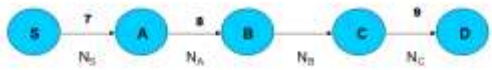

Figure 6: Data Transmission

IV. PROPOSED SCHEME

Trust Aware Routing Framework (TARF)[15] is used with USOR[2] while evaluating path towards valid destination. It identifies adversaries by their low trustworthiness and routes data through paths preventing those intruders to achieve adequate throughput. It uses following components:

- *Neighbour :* For node S, neighbouring node of S is reachable form S by only one hop wireless transmission.
- *Trust Level :* For node S, trust level of neighbour is decimal number in [0, 1], showing node S's view of neighbor's level of trustworthiness. The trust level of node is probability that neighbour of this node correctly deliver data to destination and denoted by T.

A. Trust Manager

TrustManager[15],[16] is responsible for deciding the trust level of each neighbor based on discovery of network loop. For each neighbor b of S, T_{Sb} denotes the trust level of b in S's neighborhood table.

First of all, each neighbor is given a neutral trust level. After any of those occasions happens, the individual neighbors' trust levels are altered. Trust manager sways a node to pick an alternate path when its present path as often as possible neglects to convey data to the base station.

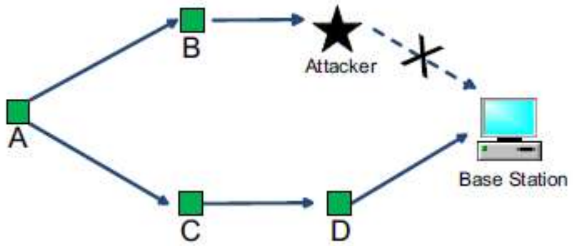

Figure7: An illustratation of how TrustManager works

Fig 7 shows an example to illustrate how TrustManager works Here, node A, B, C and D are all honest nodes and not compromised by adversaries. Node A is having node B as its current next-hop node while node B is having an attacker node as its next-hop node. The attacker node declines every packet received and hense any data packet passing through node A will not reach destination. Eventually, node A finds that the data packets it sent did not get conveyed. The Trust manager on node A begins to reduction the trust level of its present next-hop node B despite the fact that hub B is honest hub. Once that trust level results too low, node A decides to select node C as its new next-hop node. In this way node A find out a better and successful route (A - C - D - base). Disregarding the tribute of node B's trust level, the system performs better. Further, concerning the stability of routing path, once a valid node identifies a trustworthy honest neighbor as its next-hop node, it has a tendency to keep that next-hop choice without considering other apparently appealing nodes, for example, a fake base station. This tendency is due to both the preference to maintain stable routes and highly trustable nodes.

V. Experimental Results and Analysis

The performance of USOR[2] is evaluated in terms of *packet delivery ratio(PDR), packet delivery latency, and normalized control bytes.*

The ability of the proposed attack free on-demand unobservable routing protocol is confirmed via series of simulation experiments using NS-2. The number of nodes are established randomly with each node representing the individual router.

In simulation, 40 nodes are randomly distributed in network field having size of 1500mx300m rectangle field. Mobile nodes are moving by making use of random way point model. The average speed range is from 2 to 8m/s.

By using USOR protocol it has been observed that speed remains constant with packet delivery ratio as shown in fig. 8

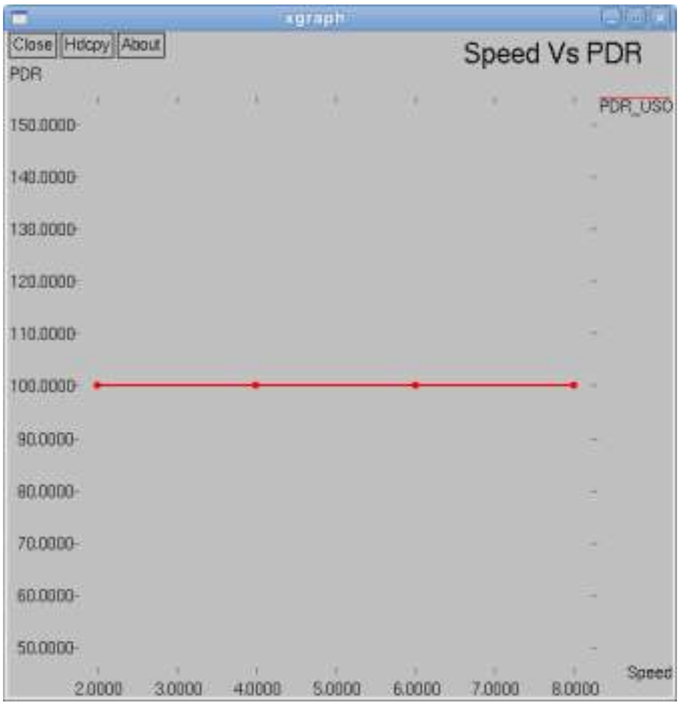

Figure 8 : Speed Vs PDR

Fig. 9 shows as speed increases delay of data transfer between nodes decreases by using USOR.

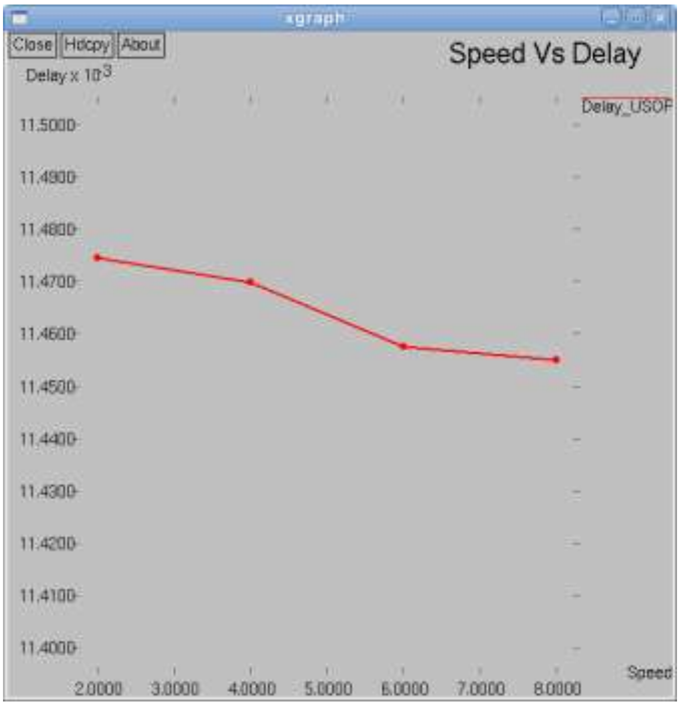

Figure 9 : Speed Vs Delay

Fig. 10 shows as speed increases normalized overhead increases and become constant after reaching threshold by using USOR.

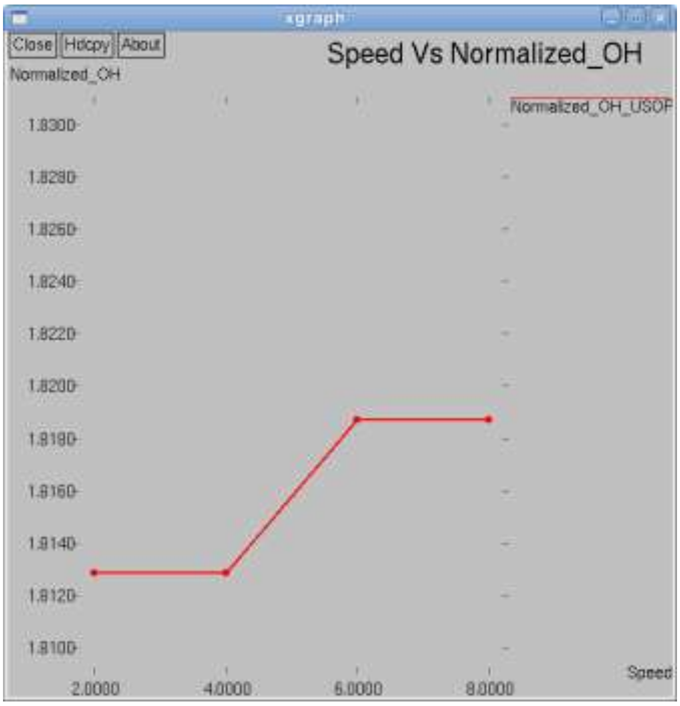

Figure 10 : Speed Vs Normalized Overhead

Fig. 11 shows as speed increases average energy of each nodes decreases by using USOR.

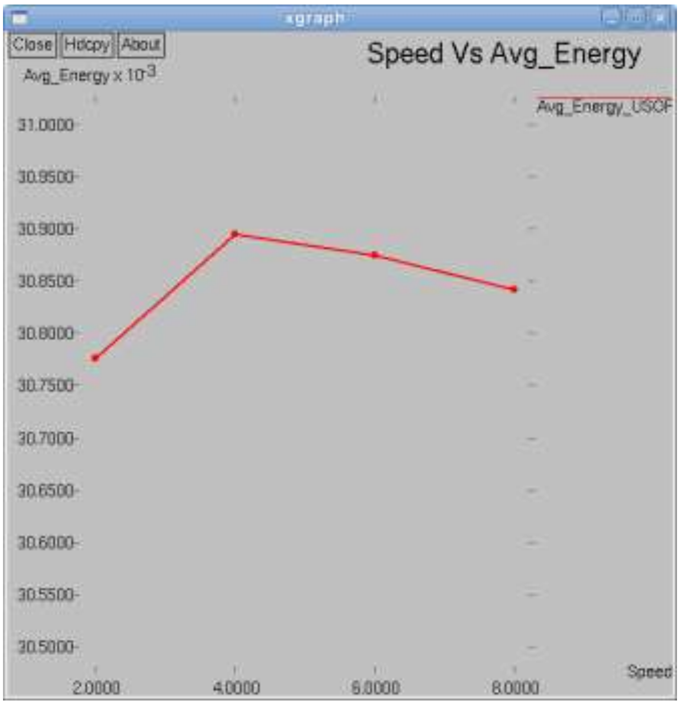

Figure 11 : Speed Vs Avg. Energy

Fig. 12 shows comparision of USOR with two other protocols like AODV and AMODV to check its efficiency in terms of packet delivery ratio(PDR). As values for protocols AMODV and AODV are same hence they are overlapped.

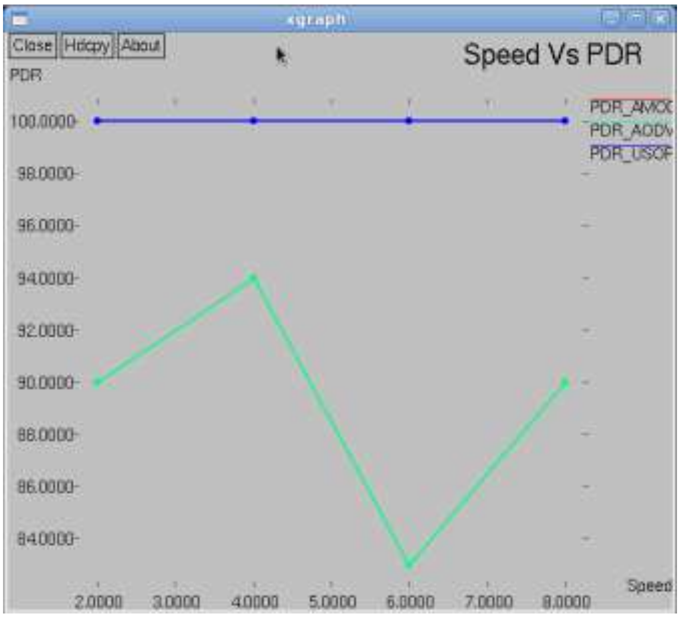

Figure 12 : Speed Vs PDR Comparision

VI. CONCLUSION

An unobservable on-demand routing protocol USOR is based on novel combination of group signature and ID-based cryptosystem for ad hoc networks. The outline of USOR offers solid protection protection, complete unlinkability, and content unobservability for ad hoc networks. The security examination exhibits that USOR not just gives solid protection assurance, additionally more safe against assaults because of node compromise. This protocol implemented on ns2 which is used to examine performance of USOR. Results demonstrates that USOR has agreeable execution in terms of packet delivery ratio, normalized control bytes.

REFERENCES

[1] A. Pfitzmann and M. Hansen, ―Anonymity, unobservability, and pseudonymity: a consolidated proposal for terminology,‖ draft, July 2000.

[2] Kui Ren, Ming Gu, and Zhiguo Wan , "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks,"IEEE Trans. on Wireless Communications, vol. 11, no. 5, pp. 1922-1932, 2012.

[3] J. Kong and X. Hong, "ANODR: aonymous on demand routing with untraceable routes for mobile ad-hoc networks," in Proc. ACM MOBIHOC' 03, pp. 291–302.

[4] Chim T.M, Dong Y, Hui C.K, Li V.O.K. and Yiu S.M. (2009) "ARMR: Anonymous Routing Protocol with Multiple Routes For Communications in Mobile Ad Hoc Networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1536– 1550.

[5] K. E. Defrawy and G. Tsudik, "ALARM: anonymous location-aided routing in suspicious MANETs," IEEE Trans. Mobile Comput., vol. 10, no. 9, pp. 1345–1358, 2011.

[6] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli, "Anonymous secure routing in mobile ad-hoc networks," in Proc. 2004 IEEE Conference on Local Computer Networks, pp. 102–108.

[7] Y. Xiao, X. Shen, and D.-Z. Du (Eds.), "A survey on attacks and countermeasures in mobile ad hoc networks", Wireless/Mobile Network Security, chapter 12, pp 1-38, Springer, 2006

[8] S. Seys and B. Preneel, "ARM: anonymous routing protocol for mobile ad hoc networks," in Proc. 2006 IEEE International Conference on Advanced Information Networking and Applications, pp. 133–137.

ISSN: 2321-8169
2356 – 2361

[9] L. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks," in Proc. 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 33–42.

[10] Y. Dong, T. W. Chim, V. O. K. Li, S.-M. Yiu, and C. K. Hui, "ARMR: anonymous routing protocol with multiple routes for communications in mobile ad hoc networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1536–1550, 2009.

[11] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks," in Proc. 2004 IEEE LCN, pp. 618–624.

[12] D. Sy, R. Chen, and L. Bao, "ODAR: on-demand anonymous routing in ad hoc networks," in 2006 IEEE Conference on Mobile Ad-hoc and Sensor Systems.

[13] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in 2005 IEEE INFOCOM.

[14] D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks," IEEE/ACM Trans. Netw., vol. 19, no. 6, pp. 1787–1796, Dec. 2011.

[15] Guoxing Zhan, Weisong Shi, and Julia Deng, 2012 "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs" IEEE Transactions on Dependable and Secure Computing, Volume 9, Issue 2, pp.184-197.

[16] W. Gong, Z. You, D. Chen, X. Zhao, M. Gu, and K. Lam, "Trust based routing for misbehavior detection in ad hoc networks," Journal of Networks, vol. 5, no. 5, May 2010.

[17] Shao-Shan Chiang, , Chih-Hung Huang, and Kuang-Chiung Chang, "A Minimum Hop Routing Protocol for Home Security Systems Using Wireless Sensor Networks," IEEE Transactions on Consumer Electronics, Vol. 53, No. 4, NOVEMBER 2007.

[18] Xufei Mao Shaojie Tang, Xiaohua Xu Xiang-Yang Li, and Huadong Ma, "Energy-Efficient Op-portunistic Routing in Wireless Sensor Networks," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 11, NOVEMBER 2011.

[19] A Novel Security Scheme for Wireless Adhoc Network, Abhijit Das Soumya Sankar Basu Atal Chaudhuri, 978-1-4577-0787-2/11 IEEE 2011.

[20] Huei-Wen Ferng,Rachmarini, D.,"A secure routing protocol for wireless sensor networks with consideration of energy efficiency/Network Operations and Management Symposium (NOMS)," 2012 IEEE .

[21] Anfeng Liu, Zhongming Zheng , Chao Zhang, Zhigang Chen, and Xuemin (Sherman) Shen,"Secure and Energy-Efficient Disjoint Multipath Routing for WSNs," IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 7, SEPTEMBER 2012.

[22] Salwa Aqeel Mahdi, Mohamed Othman, Hamidah Ibrahim, Jalil Md. Desa and Jumat Sulaiman, "PROTOCOLS FOR SECURE ROUTING AND TRANSMISSION IN MOBILE AD HOC NETWORK: A REVIEW," Journal of Computer Science 9 (5): 607-619, 2013, ISSN 1549-3636

[23] 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. 52–64, Jan.-Mar. 2003...