ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 5, November 2013

Counter Effects of Black Hole Attack on Data Transmission in Wireless Sensor Network with Multiple Base Stations

Pranjali G. Dighe, Milind B. Vaidya

Abstract- In networking, black holes refer to places in the network where incoming traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipient. The black hole attack is one of the simplest routing attacks in WSNs. In a black hole attack, the attacker swallows (i.e. receives but does not forward) all the messages he receives. As a result any information that enters the black hole region is captured. Several techniques based on secret sharing and multipath routing has been proposed in the literature to overcome black hole attacks in the network. However, these techniques are not very effective. We propose an efficient technique that uses multiple base stations deployed in the network to reduce the impact of black holes on data transmission. Our simulation results prove that our scheme achieves the 99% packet delivery success and the 100% black hole node detection.

***Index Terms*-Wireless sensor networks, black hole, multiple base stations, security.**

I. INTRODUCTION

Distributed wireless sensor networks (WSNs) have become popular in the military domains [1]. There are several problems need to be addressed in wireless sensor networks, in the area of security [8]. Black hole attacks are one such attack in WSNs. A black hole attack is an attack that is mounted by an external node on a subset of the sensor nodes (SNs) in the network. The captures node black hole nodes and re-programs them so that they do not transmit any data packets. In this paper, the re-programmed nodes are black hole nodes and the region containing the black hole nodes as a black hole region. Figure 1 shows a small circle filled with black are called as black hole and dashed red line circle called a black hole region. The techniques proposed in the literature for black hole attacks either use neighborhood interactions and message overhearing [7], [16] or secret sharing and path diversity [12],[11],[17]. Techniques based on neighborhood message interactions and overhearing work under the assumption that the SNs in the neighborhood of a black hole node are not compromised and hence can monitor and report the black hole node. However, if several SNs that are in close proximity are compromised and collude among themselves, then they can easily make neighborhood overhearing-based techniques ineffective. The path diversity and secret sharing based techniques, although better, are still not very effective.

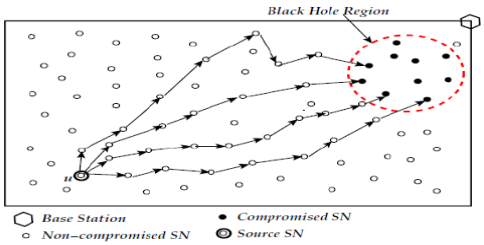

Fig 1 Success in data delivery is very low with one BS.

In fig 1 Sensor Node transmits the data towards the Base Station using four nodes disjoint paths. The figure shows that none of the packet traversing the four paths reaches the Base Station. This demonstrates that multi-path based routing can perform arbitrarily bad in the presence of black hole attacks.

II. REVIEW OF LITERATURE

Black hole attacks have been studied in the wired networks [2], [10], agent based networks [3],[6], mobil adhoc networks (MANETs) [4], [15], and wireless sensor networks [7], [11], [17]. Most of the techniques proposed in non-WSNs do not apply to the black hole problem in WSNs, because of the high computation and storage requirements. In [7] Z. Karakehayov, proposed REWARD is routing algorithm technique to detect team black-hole attacks in wireless sensor networks. In this technique, a transmitting SN performs power control to transmit a packet to more than one SN in the direction of the BS. If an SN that is on the forwarding path does not forward a packet, then its next hop neighbor on the forwarding path will identify this event and report the SN as a black hole. This scheme is very expensive for a network with n black hole nodes, for each original message, O(n) extra messages are required, which is very expensive. In [12] proposed by W. Lou, W. Liu, Y. Zhang, and Y. Fang for MANET, Security Protocol for Reliable data Delivery (SPREAD), to enhance the data confidentiality service in a mobile ad hoc network (MANET). The proposed SPREAD scheme aims to provide further protection to secret messages from being compromised (or eavesdropped) when they are delivered across the insecure network. The basic idea is to transform a secret message into multiple shares by secret sharing schemes and then deliver the shares via multiple independent paths to the destination so that even if a small number of nodes that are used to relay the message shares are compromised, the secret message as a whole is not compromised. It is more resistant to collusion attacks of up to

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 5, November 2013

a certain number of compromised nodes. In [11] W. Lou and Y. Kwon proposed a hybrid multipath scheme (H-SPREAD) to improve both the security and reliability of this task in a potentially hostile and unreliable wireless sensor network. The new scheme is based on a distributed N-to-1 multipath discovery protocol, which is able to find multiple node-disjoint paths from every sensor node to the BS simultaneously in one route discovery process. Then, a hybrid multipath data collection scheme is proposed. On the one hand, end-to-end multipath data dispersion, combined with secret sharing. In [17] Randomized Dispersive Routes. In this design, the routes taken by the shares of different packets change over time. So even if the routing algorithm become known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet. Besides randomness, the routes generated by our mechanisms are also highly dispersive and energy-efficient, making them quite capable of bypassing black holes at low energy cost. Extensive simulations are conducted to verify the validity of our mechanisms. Use of multiple base stations have been proposed in the literature to handle the flow of large amounts of heterogeneous data from the network and several optimization techniques have been designed for query allocation and base station placement [9], [18].

III. SYSTEM MODEL

One of the most effective mechanisms to ensure that data still reaches the BS is to have several BSs deployed in the network. We use Fig 2 to illustrate the effectiveness of multiple BSs. This figure is similar to previous one, but instead of only one BS at the top right corner of the network, four BSs are deployed at the four corners. This is one of the many possible ways of placing a set of BSs. As can be seen from the illustration, the packets from the SN *u* to the BS on the top right hand corner are captured by the black hole region. However, since *u* can route to the other BSs, its packets can still reach the remaining three BSs. We use this concept to provide a robust solution, with very little extra computation and message exchange overheads on the SNs in the WSN. Our technique assumes that we can place a set *B* of BSs in the network. The network is connected such that every SN can reach each $Bi \in B$. The SNs transmit copies of their data packet to each BS $Bi \in B$. Since the BSs are connected, if the packet from an SN reaches at least one of the BSs, then we assume that the packet is delivered successfully. To ensure that every SN has a route to it, each BS *Bi* uses TinyOS beaconing [8]. The beacon packet from any BS consists of: the ID of the sender of the packet, the ID of the BS from which it originated, and the hop count of the sender from the BS. BS *Bi* broadcasts the beacon packet with its ID as the sender ID as well as the BS ID, and hop count value of 0. Each neighbor that receives the beacon from *Bi*, puts its own ID as the source in the packet, increments the hop count, and broadcasts the beacon in its own neighborhood. This beaconing process creates a routing tree in the network rooted at *Bi*. As a result each SN will be part of $|B|$ routing trees. It is easy to motivate the idea that if more than one BSs were deployed far apart in the network, then the impact of the black hole region can be reduced. We note that although packet capture by black hole nodes is a concern, it can be countered with available cryptographic techniques, which ensure that the contents of a captured packet cannot be deciphered by an adversary. Consequently, successful delivery of data to the base station is a more important objective than data capture by the adversary, and this makes us to improve false positive rates of the black hole attack.

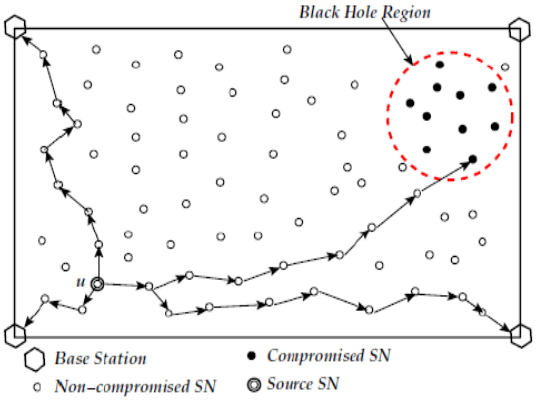

Fig 2 Data Delivery Success improves with Multiple Base Station

Protocol 1 Parents Identification at SN *u*

1. *u* receives beacons of the BSs in *B* through its neighbors.
2. for all *Ni* such that u receives beacon of $Bi \in B$ through *Ni* do
3. *u* sets Ni as its parent to reach BS *Bi.*
4. end for
5. if *u* receives the beacons from all $Bi \in B$ then
6. Create the PINFO packet, which contains the tuples *(Ni, Bi)* for each *Bi.*
7. end if
8. Encrypt the PINFO packet, using key *Kui* for each BS $Bi \in B$.
9. Transmit the encrypted PINFO to each corresponding $Bi \in B$.

Protocol 1 presents the protocol followed by an SN *u* to identify its parent in each of the routing trees using the beacon messages. After receiving the beacon messages and identifying the corresponding parents, *u* creates the PINFO packet. The PINFO packet contains the set of tuples (*Ni, Bi*) where $\{Bi \in B\}$ and *Ni* is the parent of *u* in the routing tree rooted at *Bi*. The encrypted PINFO packet is transmitted to all the BSs in the network so that the chance of reaching at least one of the BSs increases. Each SN *u* transmits a copy of its data packet to the parent in the path to each of the BSs. The data packet to a BS *Bi* is encrypted with the shared key *Kui*. Since in the worst case, each packet from *u* can potentially travel through all the nodes in the network, the message complexity of the protocol is bounded by $\mathcal{O}(n^2)$, which is the same for any packet transmission in the network.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 5, November 2013

Protocol 2 Cryptography for more secure data transmission

The Tiny Encryption Algorithm (TEA) is a cryptographic algorithm designed to minimize memory footprint and maximize speed. Despite its robustness minor extensions have been published in order to present safer encryption results. In this research, we determine the weaknesses and identify the robustness of TEA, XTEA and XXTEA algorithms in wireless sensor networks and implement them in secure framework to harden security during communication [19]. The conditions must be met in order the algorithm to bet truly ―inseparable‖ are:

The distribution of keys must have been to all nodes in a secure manner.

Each message uses a secure, unique key.

The key generation has become with a truly random cryptographic way In order to generate a set of unique, truly random keys, we use the Random Number Generator service designed and operated by the University of Trinity [20]. RANDOM.ORG's source of entropy is atmospheric noise. This noise is obtained by tuning a radio to a radio frequency that no one is using. It is then played into a workstation where a program converts it to an 8-bit mono signal at a frequency of 8 KHz. Then the first seven bits are discarded and the remaining bits are gathered together. This stream of bits has very high entropy.

IV. TECHNICAL DESCRIPTION

The system model and assumptions for our technique are as follows. The network consists of a set of randomly deployed SNs, *N={1...n}*. The network consists of a set of BSs, *B={B*1,....., *Bm}*, which are more powerful than SNs and are connected to a replenish able power source. The density of the WSN is high enough to ensure adequate connectivity so that each SN can route data packets to all the BSs in the network. The BSs are assumed to be connected to each other over a wired network. We assume that the SNs in the network can be compromised by an external adversary and programmed to analyze the packets they receive and drop them instead of forwarding them to the BSs. We refer to a compromised SN as a black hole node. The adversary is capable of compromising more than one SN in the network, thus creating one or more black hole regions. In addition, the compromised nodes are capable of colluding with other compromised nodes in their neighborhood or in other black hole regions to analyze the captured packets. We assume that the SNs in the black hole region do not perform their environment sensing tasks as they are compromised. An SN *u* shares a unique key *Kui* with each BS *Bi* $\in$ *B*. Traffic analysis can be prevented by the SNs with the use of pseudonyms, generated using schemes proposed in the literature [13]. Since the data is encrypted, analysis of the content of the data by the malicious nodes in the black hole is not possible. The malicious nodes can only perform traffic analysis of the packets they receive. The WSN is will be in a square field of dimensions 100 * 100 *m*2. The SNs are deployed randomly in the network, with the number of SNs being 200. The transmission range of the SNs was chosen to be 20m. For our simulation, the number of BSs deployed in the network are one, two, three, or four, with the positions being at the four corners of the square field, namely (0,0), (100,100), (0,100), and (100,0) respectively. To simulate different black hole sizes (hence number of black hole nodes), we chose 3 different radius for the black hole region, namely 20m, 30m, and 40m. To make the simulation more realistic, we considered two randomly placed black hole regions in the network.

Design and Implementation:-

Let, *N* is the set of randomly deployed Sensor Nodes (SNs), *N={*1,.....,*n}*.

$$\mathcal{N} = \sum_{i=1}^{n} N_i$$

Let, *B* is the set of Base Stations available in the network, which are more powerful than SNs, *B={B*1,..,.*Bm}*

$$\mathcal{B} = \sum_{i=1}^{m} B_i$$

The Sensor network represented as a graph *G*(*V*, *E*) where,

1. $\mathcal{V}=\mathcal{N} \bigcup \mathcal{B}$ where N represents the Sensor Node and B represents the Base Stations.

2. $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ represents the set of wireless links.

The network is connected such that every SN can reach each *Bi* $\in$ *B*.

The Euclidean distance between two nodes i and j by *dij* is the line segment connecting them (*ij*). In Cartesian Co-ordinates, if *i* = (*i*1, *i*2, *i*3,.....,*in*) and *j* = (*j*1, *j*2, *j*3,.....,*jn*). are two points in Euclidean n-space, then the distance from *i* to *j* or from *j* to *i* is given by,

$$d(ij) = d(ji) = \sqrt{(i_1 - j_1)^2 + (i_2 - j_2)^2 + \ldots + (i_n - j_n)^2}$$

$$= \sqrt{\sum_{x=1}^{n} (i_x - j_x)^2}$$

The distance between points *i* and *j* may have a direction, so it may be represented by another vector given by, *i* - *j={i*1 - *j*1, *i*2 - *j*2,.....,*in* - *jn}*.

Identification of the Black Hole Nodes:- *Si* denote the set of SNs identified by *Bi* as a black hole nodes, Routing tree routed at *Bi* will be given by, *{u ,v, w, x, y, z, Bi} S={Black Hole Nodes}.* Initially all SNs in the network are added to the set *Si*, *N={*1,.....,*n}*.All the BSs in B get together and create the global black hole set as,

$$\mathcal{S} = \bigcap_{i=1}^{|\mathcal{B}|} \mathcal{S}_i$$

Which are the SNs from whom none of the BSs got any data packet. This procedure performs in the network by regular time interval. Black hole node does not forward any packet to the BSs. As a result no black hole node is going to be a part of the path from any non-black hole SN to a BS.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 5, November 2013

Consequently, these nodes will not be removed from the set *Si*.

$$where, \{i|B_i \in \mathcal{B}\}$$

So all the black hole nodes will be present in the set *S*. This proves that our scheme will be able to identify all the black hole nodes.

V. PERFORMANCE EVALUATION

For evaluation, we develop framework of our protocol in a realistic setting. The WSN is deployed in a square field of dimensions 100 x 100 m2. The SNs are deployed randomly in the network, with the number of SNs being 200. The transmission range of the SNs was chosen to be 20m. For our simulation, the number of BSs deployed in the network were one, two, three, or four, with the positions being at the four corners of the square field, namely (0, 0), (100, 100),(0, 100), and (100, 0) respectively. To make the framework more realistic, we considered two randomly placed black hole regions in the network. We averaged our results over 100 topologies. For each topology, we considered 20 transmitting SNs, chosen randomly from the 200 randomly placed SNs. We compared BAMBi with the MTRP technique proposed in [19]. For the MTRP technique, we chose N = 10 and T = 6. Among other analyses, we compared the results on the basis of percentage of packets successfully delivered to the BS(s) and also the percentage of packets captured by the black hole nodes. one, two, three, or four BSs and MTRP. The MTRP technique performs worse than our technique with one BS. This can be attributed to the capture of at least N − T + 1 shares of a data packet by the black hole nodes, belonging to the two black hole regions, resulting in the failure of data delivery. As expected, the success rate falls, in general, with an increase in the radius of the black hole region. Despite the presence of two large black holes in the network, with four BSs greater than 99% of the data is delivered successfully by our technique. As expected, with an increase in the radius of the black hole region, the failure percentage for MTRP increases. With three or more BSs, the failure percentage in our technique is always lower than 7%, whereas, with MTRP the failure percentage could be more than 60%. Results showed that BAMBi identifies all the black hole nodes in the network without fail. With one BS the false positive values are high, because a large number of non-black hole nodes that are unable to reach the BS, due to disruption by the black hole nodes, are in turn identified as black hole nodes. The false positives value reduces drastically with two or more BSs, to the point where it is less than 0.5% for the case with 4 BSs. The results demonstrate the effectiveness of our technique in both delivering data to the BSs with high probability as well identifying all the black hole nodes with very little false positives.

Route 1	Hop Count : 5			
Nodes	ID	ENC-ID	Delivery	Packet Recieved
n5	0005-SN	chzljNY9EhA=	---	---
n11	0011-SN	th66z08AQUk=	Success	chzljNY9EhA=@n11@1
n17	0017-SN	CDwUgm1kKzY=	Success	chzljNY9EhA=th66z08AQUk=@n17@1
n13	0013-SN	As5KHuib9+o=	Success	chzljNY9EhA=th66z08AQUk=CDwUgm1kKzY=@n13@1
n19	0019-SN	9DC/DcrdoV4=	Success	chzljNY9EhA=th66z08AQUk=CDwUgm1kKzY=As5KHuib9+o=@n19@1
n20	0020-SN	0OE6aiHhI9Q=	Success	chzljNY9EhA=th66z08AQUk=CDwUgm1kKzY=As5KHuib9+o=9DC/DcrdoV4=@n20@1

Fig 3 XXTEA algorithm output

Route 1	Hop Count : 3		
Nodes	ID	Delivery	Packet Recieved
n11	012345	---	---
n17	012345	Success	012345@n17@1
n24	$$$$$$	Success	012345012345@n24@1
n20	012345	Failed	

Route 2	Hop Count : 3		
Nodes	ID	Delivery	Packet Recieved
n11	012345	---	---
n7	012345	Success	012345@n7@1
n3	012345	Success	012345012345@n3@1
n21	012345	Success	012345012345012345@n21@1

Route 3	Hop Count : 3		
Nodes	ID	Delivery	Packet Recieved
n11	012345	---	---
n5	012345	Success	012345@n5@1
n0	012345	Success	012345012345@n0@1
n22	012345	Success	012345012345012345@n22@1

Route 4	Hop Count : 2		
Nodes	ID	Delivery	Packet Recieved
n11	012345	---	---
n15	012345	Success	012345@n15@1
n23	012345	Success	012345012345@n23@1

Route 5	Hop Count : 1		
Nodes	ID	Delivery	Packet Recieved
n25	$$$$$$	---	---
n20	012345	Success	$$$$$$@n20@1

Route 6	Hop Count : 4		
Nodes	ID	Delivery	Packet Recieved
n25	$$$$$$	---	---
n13	012345	Success	$$$$$$@n13@1
n7	012345	Success	$$$$$$012345@n7@1
n3	012345	Success	$$$$$$012345012345@n3@1
n21	012345	Success	$$$$$$012345012345012345@n21@1

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 5, November 2013

Route 7	Hop Count : 4		
Nodes	ID	Delivery	Packet Recieved
n25	$$$$$$	---	---
n13	012345	Success	$$$$$$@n13@1
n7	012345	Success	$$$$$$012345@n7@1
n1	012345	Success	$$$$$$012345012345@n1@1
n22	012345	Success	$$$$$$012345012345012345@n22@1

Route 8	Hop Count : 4		
Nodes	ID	Delivery	Packet Recieved
n25	$$$$$$	---	---
n13	012345	Success	$$$$$$@n13@1
n12	012345	Success	$$$$$$012345@n12@1
n16	012345	Success	$$$$$$012345012345@n16@1
n23	012345	Success	$$$$$$012345012345012345@n23@1

+

Total Routes	8
Failed	1
Fake Success	4
Success	3

Fig 4 Black Hole and False Black Hole Attack Output

VI. CONCLUSION

In this paper, we propose a technique to effectively mitigate the adverse effects of black hole attacks on WSNs. This technique based on the deployment of multiple base stations in the network and routing of copies of data packets to these base stations. Our solution is highly effective and requires very little computation and message exchange in the network, thus saving the energy of the SNs. In the future, we wish to identify the optimal number of BSs and their positions and improve the message complexity of the protocol.

REFERENCES

[1] Akyildiz, W.Su, Y.sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A survey. Computer Networks, 38(4):393–422, 2002.

[2] E. Cooke, M. Bailey, Z. M. Mao, D.Watson, and F. Jahanian. Toward understanding distributed black hole placement. In Proc of ACM CCS Workshop on Rapid Malcode, pages 54–64. ACM Press, October 2004.

[3] J. Czyzowicz, D. Kowalski, E. Markou, and A. Pelc. Searching for a black hole in tree networks. In Proceedings of 8th International Conference on Principles of Distributed Systems (OPODIS 2004), pages 34–35, 2004. Also: Springer LNCS vol. 3544, pages 67-80, also to appear as "Searching for a Black Hole in Synchronous Tree Networks" in Combinatorics, Probability and Computing.

[4] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," IEEE Net., vol. 13, no. 6, pages 24-30, Nov./Dec. 1999.

[5] Advanced Encryption Standard (AES), ser. FIPS PUB 197, November 2001.

[6] S. Dobrev, P. Flocchini, G. Prencipe, and N. Santoro. Searching for a black hole in arbitrary networks: Optimal mobile agent protocols. In Proc. of 21st ACM Symposium on Principles of Distributed Computing (PODC'02), 153-162, 2002.

[7] Z. Karakehayov. Using REWARD to detect team black-hole attacks in wireless sensor networks. In ACM Workshop on Real-World Wireless Sensor Networks, 2005.

[8] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2–3):293–315, September 2003.

[9] S. Kim, J.-G. Ko, J. Yoon, and H. Lee. Multiple-objective metric for placing multiple base stations in wireless sensor networks. In Proceedings of the International Symposium on Wireless Pervasive Computing, pages 627–631, February 2007.

[10] R. Kompella, J. Yates, A. Greenberg, and A. Snoeren. Detection and localization of network black holes. In Proceedings of IEEE INFOCOM, pages 2180–2188, 2007.

[11] W. Lou and Y. Kwon. H-SPREAD: A hybrid multipath scheme for secure and reliable data collection in wireless sensor networks. IEEE Transactions on Vehicular Technology, 55(4):1320–1330, 2006.

[12] W. Lou, W. Liu, Y. Zhang, and Y. Fang. SPREAD: Enhancing data confidentiality in mobile ad hoc networks. In IEEE INFOCOM, volume 4, pages 2404–2413, 2004.

[13] S. Misra and G. Xue. Efficient anonymity schemes for clustered wireless sensor networks. Intl. Journal of Sensor Networks, 1(1):50–63, 2006.

[14] Y. Zhang, W. Lee, Intrusion detection in wireless ad-hoc networks, in: Proceedings of MobiCom '00, August 2000, pp. 275–283.

[15] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and E. Kendall. Prevention of cooperative black hole attack in wireless ad hoc networks. In Proceedings of the Intl. Conf. on Wireless Networks, 2003.

[16] S. Roy, S. Singh, S. Choudhary, and N. Debnath. Countering sinkhole and black hole attacks on sensor networks using dynamic trust management. In IEEE Symposium on Computers and Communications, pages 537–542, 2008.

[17] T. Shu, S. Liu, and M. Krunz. Secure data collection in wireless sensor networks using randomized dispersive routes. In IEEE INFOCOM, pages 2846–2850, 2009.

[18] B. Yu, B. Xiao, Detecting selective forwarding attacks in wireless sensor networks, in: Proceedings of the Second International Workshop on Security in Systems and Networks (IPDPS 2006 Workshop), 2006, pp. 1–8.

[19] D. Wheeler and R. Needham. "TEA, a Tiny Encryption Algorithm. " 1995. Springer-Verlag.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 5, November 2013

[20] L. Foley, S. Wilson, "Analysis of an On-line Random Number Generator", Trinity College Dublin, http://www.random.org, (Accessed 8 April 2011).

[21] P. Dighe, M. Vaidya, "Deployment of Multiple Base stations to counter effects of Black Hole on data transmission in Wireless Sensor Network", in: International Journal of Engineering and innovative Technology (IJEIT), 2012,Vol-1,Issue-4, pp. 1–6.

AUTHOR'S PROFILE

First Author 1M.E. Student of Computer, Pune.
Second Author [2]Assistant Professor AVCOE, Sangamner.