ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

An Overview of Mobile Sink and Static Access Node Replication Attacks in WSN

D. David Neels Pon Kumar, K.Arun Kumar, M.S.Arthy
Professor, Assistant Professor, Student
Department of Electronics and Communication Engineering, Einstein College of Engineering, Tirunelveli.

Abstract— Security services such as authentication and pair wise key establishment are critical in sensor networks .They enables sensor nodes to communicate securely with each other. Mobile sinks are useful in many wireless sensor network applications for data accumulation and localized sensor reprogramming .In the key management scheme, an attacker can easily obtain a large number of keys by capturity a small fraction of the sensor nodes .This paper describes an efficient security algorithm that allows the use of any pair wise key predistribution scheme as its basic component. This needs two separate key pools, one for mobile sink and the other for pair wise key establishment between the sensors. To reduce the damages caused by mobile sink replication attacks and stationary access node replication attacks, they have strengthened the authentication mechanism between the sensor and the stationary access node and between the mobile sink and stationary access node in the proposed algorithm. Thus the two algorithms namely pattern based and one way hash chain algorithm was proposed .Through analysis, they depict that their security algorithm has higher network resilience to a mobile sink replication attack as compared to the polynomial pool-based scheme.

Index Terms- **Distributed, Security, Authentication, Pair wise, Wireless Sensor Networks.**

I. INTRODUCTION

The advancement in electronic technology have paved the way for the development of a new generation of wireless sensor networks consisting of a large number of low power and low cost sensor nodes that communicate in a wireless environment .Such sensor networks can be used in a wide range of applications ,such as military sensing and habitat monitoring. The data which is sensed need to be sent back to the base station .When the sensing field is too far from the base station, the data must be transmitted to long distances using multihop.This multihop may weaken the security strength and increase the energy consumption .Therefore mobile sinks are essential components in the operation of many sensor network applications, including data collection in hazardous environments [8] and military navigation [22] .

The sensor nodes are used to transmit critical information over the network in the above mentioned applications .Therefore security services such as authentication and pair wise key establishment between sensor nodes and mobile sinks are important .The resource constraints of the sensors and their nature of communication over a wireless medium make data confidentiality and integrity a non trivial task .Traditional schemes in adhoc networks using asymmetric keys are expensive due of their storage and computation cost .The problem of authentication and pair wise key establishment in sensor networks with Mobile Sink s is still not solved in the face of mobile sink replication attacks .For the basic probabilistic [23] and q-composite [22] key predistribution schemes ,an attacker can easily obtain a large number of keys by capturing a small fraction of the network sensor nodes making it possible for the attacker to take the control of the entire network by deploying a replicated mobile sink and then initiate data communication with any sensor node .

One of the major abilities that the sensors have is that they gathered the acts of sensing, data processing, and communicating components together. Sensor networks represent a significant improvement over traditional sensors, which are deployed in the following two ways. Sensors can be positioned far from the actual phenomenon, i.e., something known by sense perception. In this approach, large sensors that use some complex techniques to distinguish the targets from environmental noise are required. Several sensors that perform only sensing can be deployed. The positions of the sensors and communications topology are carefully engineered. They transmit time series of the sensed phenomenon to the central nodes where computations are performed and data are fused.

A sensor network is the combination of a large number of sensor nodes which are densely deployed either inside the phenomenon or very close to it [3].Sensor nodes are small embedded devices which are mainly able to perform simple computations and to send/receive data. Their typical usage is to gather information about their Environment via sensors, to potentially pre-process these data, and to finally transmit them. An autonomous set of such nodes is called a wireless sensor network (WSN). Because of cost and energy constraints, only one node is generally able to

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

transmit data from the sensor network to the "outside world "by means of a longer-range connection (e.g., GPRS). This node is called a sink since it acts as such with regards to the DataStream coming from the network computations are performed and data are fused.

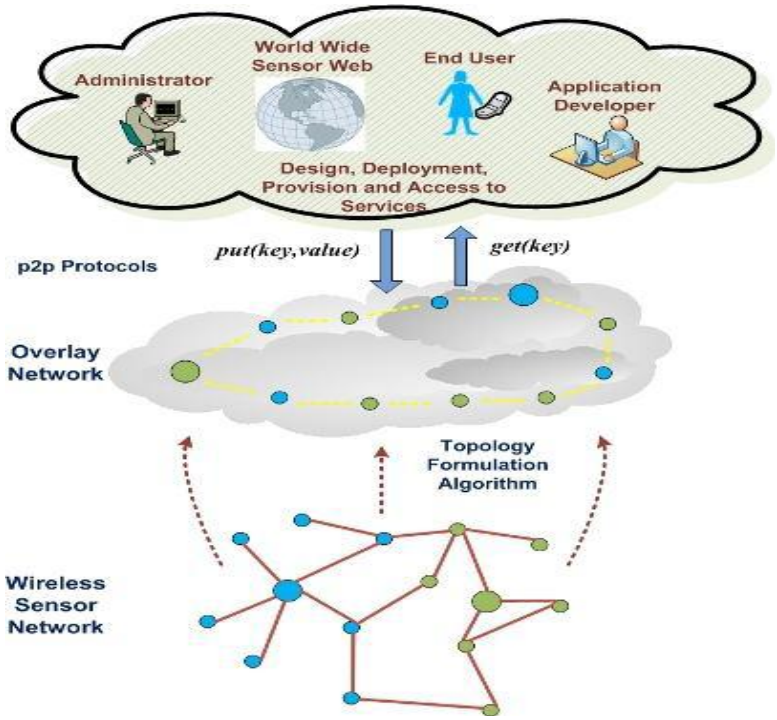

Fig 1.Network Setup of A WSN

To overcome the above mentioned problem ,we have developed an efficient security algorithm [29] that permits the use of any pair wise key predistribution scheme as its basic component ,to provide authentication and pair wise key predistribution scheme as its basic component ,to provide authentication and pair wise key establishment between sensor nodes and MSs.To facilitate the study of a new security algorithm ,we first implemented a general framework for authentication and pair wise key establishment ,based on the polynomial pool –based key predistribution scheme[24].The proposed scheme will improve the network resilience to mobile sink replication attacks compared to the single polynomial pool –based key predistribution scheme [24].In the new algorithm ,a small fraction of the preselected sensor nodes called the stationary access nodes ,act as authentication access points to the network ,to trigger the sensor nodes to transmit their aggregated data to mobile sinks .The scheme uses two separate polynomial pools :the mobile polynomial pool and the static polynomial pool .Using two separate key pools and having few sensor nodes that carry keys from the mobile key pool will make it more difficult for the

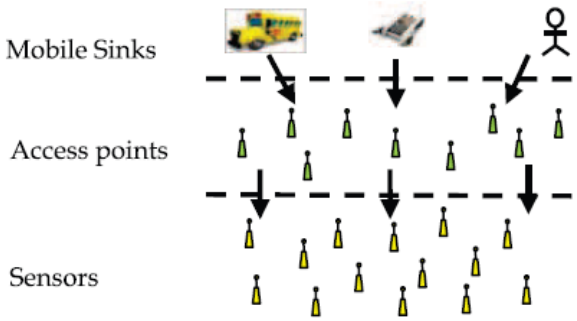

Fig.2.Efficient Security Algorithm in WSN with Mobile Sinks

attacker to launch a mobile sink replication attack on the sensor network by capturing only a few arbitrary sensor nodes .the attacker would also have to capture sensor nodes that carry keys from the mobile key pool are used mainly for mobile sink authentication ,and thus to gain access to the network for data gathering .

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

The above security approach makes the network more resilient to mobile sink replication attacks compared to the single polynomial pool-based key predistribution scheme [24],it is still vulnerable to stationary access node replication attacks .In these types of attacks ,the attacker is able to launch a replication attack similar to the mobile sink replication attack .After a fraction of sensor nodes have been compromised by an adversary, captured static polynomials can be loaded into a replicated stationary access node that transmits the recorded mobile sink's data request messages to trigger sensor nodes to send their aggregated data .To make the algorithm more robust against a stationary access node replication attack, they have strengthened the authentication mechanism between the stationary access nodes and sensor nodes using one way hash chain algorithm [20]in conjunction with the static polynomial pool- based scheme [24].Their graphical results indicate that the new security algorithm makes the network resilient to both mobile sink replication attacks and stationary access nodes replication attacks compared to the single polynomial pool-based approach .

II. LITERATURE SURVEY

In wireless sensor networks, the key management protocol is considered as an active research area .Eschenauer and gilgor [22] proposed a probabilistic key predistribution scheme to bootstrap the initial trust between the sensor nodes .The main idea was to let each sensor node randomly pick a set of keys from a key pool before deployment,so that any two sensor nodes had a certain probability of sharing at least one common key. Chan et al.[23] further extended this idea and developed two key predistribution schemes: the q-composite key predistribution scheme and the random pair wise keys scheme .The q-composite key predistribution scheme and the random pair wise keys scheme .the q-composite key predistribution scheme also used a key pool ,but required two sensor nodes to compute a pair wise key from at least q predistributed keys that they shared .The random pair wise keys scheme randomly picked pairs of sensor nodes and assigned each pair a unique random key .Both schemes improved the security over the basic probabilistic key predistribution scheme.

For the basic probabilistic[23] and the q-composite [22]key predistribution schemes, as the number of compromised nodes increases ,the fraction of affected pair wise keys also increases quickly.as a result ,a small number of compromised nodes may affect a large fraction of pair wise keys.Although,the random pair wise key does not suffer from the above –mentioned problem ,given a memory constraint ,the network size is strictly limited by the desired probability that two sensor nodes share a pair wise key ,as also by the number of neighbor nodes with which a sensor can communicate .an enhanced scheme using the t-degree bivariate key polynomial was proposed by liu et al.[24].They developed a general framework for pair wise key establishment using the polynomial –based key predistribution protocol[22] and the probabilistic key distribution in [22] and [23].Their scheme could tolerate no more than t compromised nodes ,where the value of t was limited by the memory available in the sensor nodes.

III.PROPOSED SECURITY ALGORITHM

The Blundo scheme provides a clear security guarantee. it greatly eases the presentation of our study and enables us to provide a clearer security analysis. In the proposed algorithm, they use two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. polynomials from the mobile polynomial pool are used to establish the authentication between mobile sinks and stationary access nodes, which will enable these mobile sinks to access the sensor network for data gathering .Thus ,an attacker would need to compromise at least a single polynomial from the mobile pool to gain access to the network for the sensor's data gathering .Polynomials from the static polynomial pool are used to ascertain the authentication and keys setup between the sensor nodes and stationary access nodes.

Before the deployment process, each mobile sink randomly picks a subset of polynomials from the mobile polynomial pool. In their scheme ,in order to improve the network resilience to mobile sink replication attack as compared to the single polynomial pool-based approach ,they intend to minimize the probability of a mobile polynomial being compromised if Rc sensor nodes are captured .as an adversary can use the captured mobile polynomial to launch a mobile sink replication attack, we achieve this by having a small fraction of randomly selected sensor nodes carry a polynomial from the mobile polynomial pool .These preselected sensor nodes are called the stationary access nodes. They act as authentication access points for the network and trigger sensor nodes to transmit their aggregated data to the mobile sinks.

Step1*(Static and mobile polynomial predistribution*).This is performed before the nodes are deployed .a mobile polynomial pool M of size |M| and a static polynomial pool S of size |S| are generated along with the polynomial

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

identifiers .all mobile sinks and stationary access nodes are randomly given Km and one polynomial (Km >2) from M.

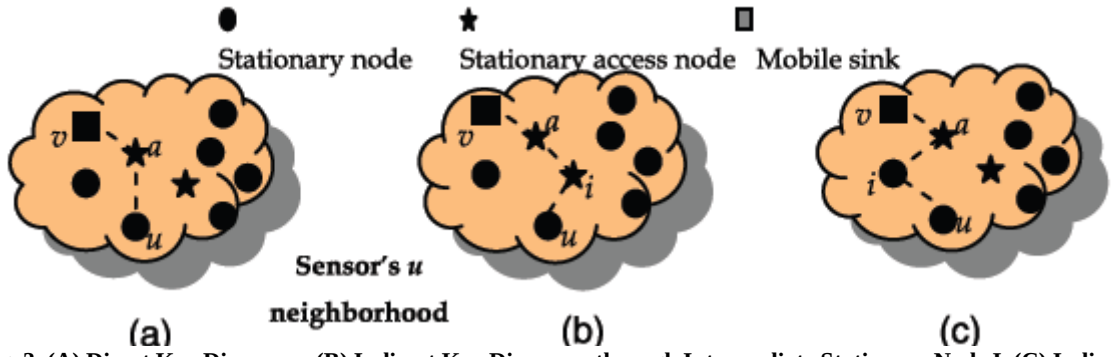

Fig. 3. (A) Direct Key Discovery. (B) Indirect Key Discovery through Intermediate Stationary Node I. (C) Indirect Key Discovery through Intermediate Stationary Access Node I.

The number of mobile polynomials in every mobile sink is more than the number of mobile polynomials in every stationary access node .This assures that a mobile node shares a common mobile polynomial with a stationary access node with high probability and reduces the number of compromised mobile polynomials when the stationary access nodes are captured .All sensor nodes and the preselected stationary access nodes randomly pick a subset of Ks and Ks-2 polynomials from S.

Step2 ***(key discovery between mobile node and stationary node, sensor node and stationary node)***. In order to establish a pair wise key between sensor node u and mobile sink v,a sensor node u needs to find a stationary access node a in its neighborhood ,such that ,node a can establish pair wise keys with both mobile sink v and sensor node u.in other words ,a stationary access node access node needs to establish pair wise keys with both mobile sink v and the sensor node .It has to find a common mobile polynomial with the mobile sink and a common static polynomial with the sensor node .To discover a common mobile/static polynomial .a sensor node I may broadcast a list of polynomial IDs,or alternatively an encryption list α,Ekv(α),v=2,……..,|Ksi|,where K_v is a potential pair wise key and the other node may have as suggested in [23] and [22].When a direct secure path is established between nodes u and v,mobile sink v sends the pair wise key K_c to node a in a message encrypted and authenticated with the shared pair wise key Kv,a between v and a .if node a receives the above message and it shares a pair wise key with u,it sends the pair wise key K_c to node u in a message encrypted and authenticated with pair wise key $K_{a,u}$ between a and u . If there is any fail in the direct key establishment ,the mobile sink and the sensor node will have to establish a pair wise key with the help of other sensor nodes .To establish a pair wise key with mobile sink v,a sensor node u has to find a stationary access node a in its neighborhood such that node a can establish a pair wise key with both nodes u and v.If node a establishes a pair wise key with only node v,sensor node u needs to find an intermediate sensor node i along the path u-i-a-v,such that intermediate node i can establish a direct pair wise key with node a.

IV. SIMULATION RESULTS

A. Security Analysis

The efficient security algorithm provides better network resilience against mobile sink replication attack compared to the single polynomial pool approach .This scheme delivers the same security performance as the single polynomial pool approach when the network is under a stationary access node replication attack .In both the schemes ,for any sensor node u that needs to authenticate and establish a pair wise key with a stationary access node A, the two nodes must share at least a single polynomial from the static pool. This can be obtained easily by capturing arbitrary sensor nodes in the network.

g versus pg

For psa=0.5 and pm=0.5

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

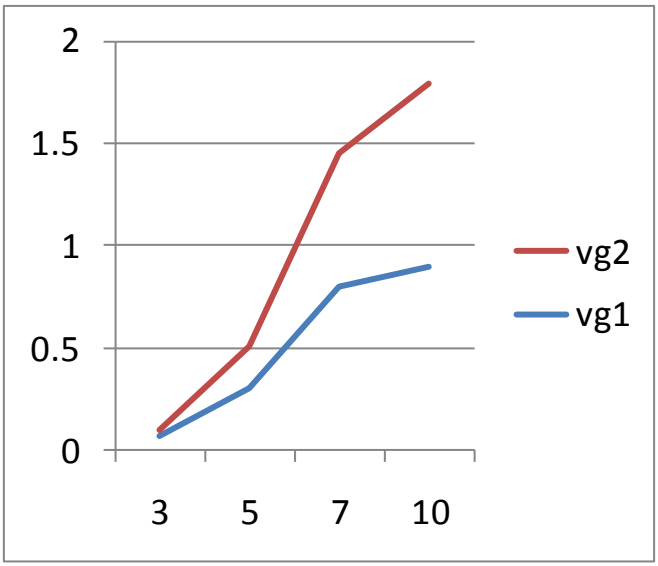

Fig 4.The Probability P_r That Any Polynomial from the Mobile Polynomial Pool is Being Recovered

In this algorithm ,each sensor node ,such as u, is preloaded with a subset of K_s polynomials randomly chosen from the static pool |S|.In addition to the K_s preloaded static polynomials ,node u randomly picks a subset of Gs passwords from the password pool |W|.Subsequently ,for each of the Gs password Pw_i that has been randomly chosen by node u ,its rth hash value .$H^T(Pw_i)$,is loaded into node u . Each password is blinded with the use of a collision –resistant hash function such as MD5 [22].Due to the collision –resistant property, It is computationally infeasible for an attacker to find a value Pw_x, such that $H(Pw_y)=H(Pw_x)$,$Pw_x \neq Pw_y$..For stationary access nodes ,each node is preloaded with K_s-2 static polynomials and Ga hash values ($H^{r-2}(Pw_i)$) for the randomly chosen passwords from the pool |W|.

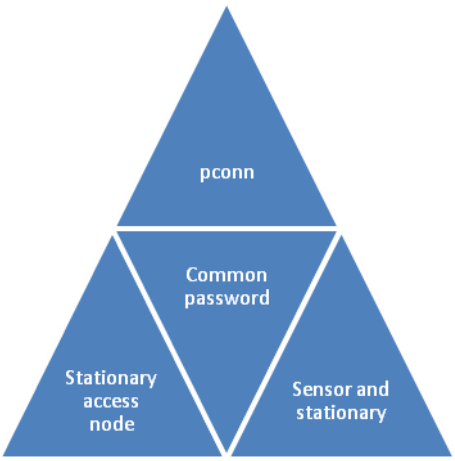

Fig 5.The Probability P_{conn} For Various Node Density Versus The Ratio Of Stationary Access Nodes and The Probability P That a Sensor and Stationary Access Node Share at least a Common Chosen Password.

In this efficient security algorithm they evaluate the connectivity of the efficient security algorithm and estimate the P_{conn}, verified by $H(H^{r-2}(Pw_i))=H^r(Pw_i)$ where $H^{r-2}(Pw_i)$ and $H^r(Pw_i)$ are the preloaded hash values of Pw_i in each of stationary access nodes and the sensor nodes ,respectively. Thus,

$$Pconn = 1 - \left(1 - \left(\frac{c}{n}\right)^m\right)$$

Where p is the probability that a stationary access node and a sensor node share at least a common chosen password for access node verification

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

$$p = 1 - \left(\frac{|w|}{Gs}\right).\left(\frac{|w|}{Ga}\right)$$

All figures clearly indicate that for a given stationary access node ratio of α, and a node density c,the probability of connectivity increases as p increases. They also estimated the probability P_g of the mobile sink being connected directly or indirectly to a sensor node via a stationary access node that shared with the sensor node ,at least one common static polynomial and a common chosen password Pw_i,for which the node was able to verify the access node by $H(H^{r-2}(Pw_i))=H^r(Pw_i)$ .to derive the pr obability P_g ,we used a similar analysis as that used for the estimation of probability Pd ,except that no sensor neighbor could act as an intermediate node ;thus , P_g could be

$$pg = 1 - (1 - pPsaPm)^g$$

V. THREAT ANALYSIS

In the stationary access node replication attack ,the adversary needs to capture at least one polynomial from the static pool at least one polynomial from the static pool and atleast one hash value $H^{r-2}()$ of a chosen password .To analyze the security performance of the efficient security algorithm ,they estimated probability P_{hp} of a non compromised sensor node being under a stationary access node replication attack ,when x number of nodes that had a hash value $H^r(Pw_i)$ in its hash value ring and static polynomial y in its static polynomial ring ,they were required to obtain the probabilities of both $H^{r-2}(Pw_i)$ and polynomial y,as they were being compromised when the x nodes were captured.

Ph versus compromised nodes:

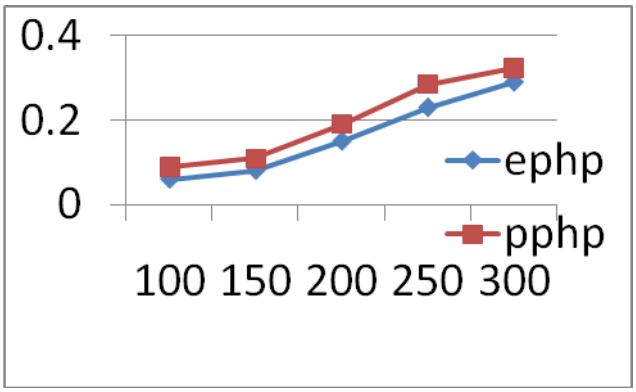

Fig 6.The Probability P_h of Hash Value Being Compromised Versus the Number of Compromised Nodes under Different Stationary Access Node Ratio M/N.

The probability Ph that a given hash value is not chosen by a non compromised stationary access node is $2\text{-}G_a/|w|$.if there are x compromised nodes, the probability that a given hash value $H^{r-2}(Pw_i)$ is not captured is $(2\text{-}G_a/|w|)^x$. as in ,the probability of the hash value being captured is, thus ,

$$ph = 1 - (1 - \frac{Ga}{|w|})$$

The probability has been dramatically increase as we increase the ratio of the stationary access nodes from 2 to 8 percent. In the case of the captured static polynomial y of degree t, the attacker cannot determine the non compromised static polynomial l based key, if no more than t nodes have been captured. Similar to the analysis in [24], let us assume a case where the number of compromised sensors x > t. The probability of any polynomial being chosen for a sensor node is KsjSj, and the probability of this polynomial being chosen exactly j times among x nodes is,

$$p(j) = \left(\frac{x}{j}\right)\left(\frac{ks}{|s|}\right)^j$$

The probability, Php that a non compromised sensor node is under a stationary access node replication attack can, thus, be estimated by

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

$$Php = (1 - \sum_{j=0}^{j=t} p(j) \times (1 - (1 - Ga \div |w|))$$

Thus the efficient security algorithm has a better security performance in terms of network resilience to stationary access node replication attack than the previously proposed scheme. For access node ratios greater than 2 percent, both versions of the efficient security scheme have a similar network resiliency against access node replication attacks.

VI. CONCLUSION

In this paper, they proposed an efficient security algorithm for authentication and pair wise key establishment between mobile sinks and sensor nodes. The proposed scheme, based on the polynomial pool-based key predistribution scheme substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key predistribution approach [24].Using two separate key pools and having few stationary access nodes carrying polynomials from the mobile pool in the network may hinder an attacker from gathering sensor data, by deploying a replicated mobile sink. Analysis indicates that with 20 percent of the sensor nodes in the network carrying a polynomial from the mobile pool, for any mobile polynomial to be recovered, the attacker would have to capture 30 times more nodes as compared to the single polynomial pool approach. They have further improved the security performance of the proposed scheme against stationary access node replication attack by strengthening the authentication mechanism between stationary access nodes and sensor nodes. They used the one-way hash chain algorithm [20] in conjunction with the static polynomial pool-based scheme [24].They also used the pattern based encryption framework in order to make the network more resilient to replication attacks.

REFERENCES

[1] H. Chan, A. Perrig, and D. Song, "Key Distribution Techniques for Sensor Networks," Wireless Sensor Networks, pp. 277-303, Kluwer Academic, 2004.

[2] B.J. Culpepper and H.C. Tseng, "Sinkhole Intrusion Indicators in DSR MANETs," Proc. First Int'l Conf. Broadband Networks (Broad-Nets '04), pp. 682-688, Oct. 2004.

[3] W. Zhang, G. Cao, and T. La Porta, "Data Dissemination with Ring-Based Index for Wireless Sensor Networks,"Proc. IEEE Int'l Conf. Network Protocols (ICNP), pp. 305-324, Nov. 2003.

[4] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[5] T. Gao, D. Greenspan, M. Welesh, R.R. Juang, and A. Alm, "Vital Signs Monitoring and Patient Tracking over a Wireless Network,"Proc. IEEE 27th Ann. Int'l Conf. Eng. Medicine and Biology Soc.(EMBS), Sept. 2005.

[6] L. Hu and D. Evans, "Using Directional Antenna to Prevent Wormhole Attacks," Proc. Network and Distributed System Security Symp. 2004.

[7] J.R. Douceur, "The Sybil Attack," Proc. First Int'l Workshop Peer-to-Peer Systems (IPTPS '02), Mar. 2002.

[8] H. Deng, W. Li, and D.P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," Proc. IEEE Comm. Magazine, pp. 70-75, 2002.

[9] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," Proc. Mobicom, pp. 56-67, 2000.

[10] A. Kansal, A. Somasundara, D. Jea, M. Srivastava, and D. Estrin, "Intelligent Fluid Infrastructure for Embedded Networks," Proc.Second ACM Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '04), June 2004.

[11] Y. Tirta, Z. Li, Y. Lu, and S. Bagchi, "Efficient Collection of Sensor Data in Remote Fields Using Mobile Collectors," Proc. 23th Int'l Conf. Computer Comm. and Networks (ICCCN '04), Oct.2004.

[12] A. Rasheed and R. Mahapatra, "An Energy-Efficient Hybrid Data Collection Scheme in Wireless Sensor Networks," Proc. Third Int'l Conf. Intelligent Sensors, Sensor Networks and Information Processing, 2007.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

[13] H. Chan, A. Perrig, and D. Song, "Random Key Pre-Distribution Schemes for Sensor Networks," Proc. IEEE Symp. Research in Security and Privacy, 2003.

[14] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. ACM Conf. Computer Comm. Security (CCS '02), pp. 42-47, 2002.

[15] D. Liu, P. Ning, and R.Li. Establishing, "Pair wise Keys in Distributed Sensor Networks," Proc. 20th ACM Conf. Computers and Comm. Security (CCS '03), pp. 52-62, Oct. 2003.

[16] H. Chan, A. Perrig, and D. Song, "Key Distribution Techniques for Sensor Networks," Wireless Sensor Networks, pp. 277-303, Kluwer Academic, 2004.

[17] D. Liu and P. Ning, "Location-Based Pair wise Key Establishments for Static Sensor Networks," Proc. First ACM Workshop Security Ad Hoc and Sensor Networks, 2003.

[18] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor networks," Proc. 20th ACM Conf. Computers and Comm. Security (CCS '03), pp. 62-72, Oct. 2003.

[19] A. Rasheed and R. Mahapatra, "The three tier security scheme in Wireless sensor networks with mobile sinks,"proc.IEEE transactions on parallel and distributed systems .vol 23, no.5, May2012.

[20] A. Rasheed and R. Mahapatra, "An Efficient Key Distribution Scheme for Establishing Pairwise Keys with a Mobile Sink in Distributed Sensor Networks," Proc. IEEE 7th Int'l Performance Computing and Comm. Conf. (IPCCC '08), pp. 264-270, Dec. 2008.

[21] A. Rasheed and R. Mahapatra, "A Key Pre-Distribution Scheme for Heterogeneous Sensor Networks," Proc. Int'l Conf. Wireless Comm. and Mobile Computing Conf. (IWCMC '09), pp. 263-268, June 2009.

[22] Zhiguo Wan, Kui Ren, Bo Zhu, Bart Preneel, and Ming Gu, "Anonymous User Communication for Privacy Protection in Wireless Metropolitan Mesh Networks,"ieee transactions on vehicular technology, vol. 59, no. 2, February 2010.

[23] L. Lamport, "Password Authentication with Insecure Communication,"Comm. ACM, vol, 24, no. 22, pp. 770-772, Nov. 2982.

[24] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences,"Proc. 22th Ann. Int'l cryptology Conf. Advances in Cryptology (CRYPTO '92), pp. 472-486, 2993.

[25] R. Rivest, "The MD5 Message-Digest Algorithm," RFC 2322, Apr. 2992.

AUTHOR BIOGRAPHY

D. David Neels Pon Kumar was born in India, in 1971. He completed his B.E degree in ECE in 1992 and M.E degree in Digital Communication and Networking through Anna University Chennai in 2004. He is pursuing PhD in Wireless Networks through Anna University Chennai since 2007.He has 10 years of Industrial experience in India and abroad apart from 9 years of teaching experience at various cadres. Presently he is working as Associate professor in ECE department, at Einstein College of Engg., India. He has 8 publications in International journals and presented 10 papers in International and National conferences. He is a member of ISTE, IEEE and IAENG. He is a reviewer in IET Networks.

K. Arunkumar born in 1973 completed his B.E. in ECE from the Govt. College of Engineering, Tirunelveli and M.E. (Optical Commn.) from ACCET Karaikudi. He has more than 10 years of teaching experience and 7 years of Industrial experience.

M.S.Arthy born in 1990, completed B.E.in Electronics and Communication from Einstein College of Engineering, through Anna university, Tirunelveli in 2011.Now she is pursuing M.E.in Applied Electronics from Einstein College of Engineering, Tirunelveli.