Resilience Against Node Capture Attack using Asymmetric Matrices in Key Predistribution Scheme in Wireless Sensor Networks

Shaila K*, S H Manjula*, Thriveni J*, Venugopal K R* and L M Patnaik**
* Department of Computer Science and Engineering
University Visvesvaraya College of Engineering, Bangalore University, Bangalore 560 001
** Vice Chancellor, Defence Institute of Advanced Technology, Pune, India
shailak17@gmail.com

Abstract — Wireless Sensor Networks (WSN) usually consists of a large number of tiny sensors with limited computation capability, memory space and power resource. WSN's are extremely vulnerable against any kind of internal or external attacks, due to several factors such as resource constrained nodes and lack of tamper-resistant packages. To achieve security in Wireless Sensor Networks, it is important to encrypt messages sent among sensor nodes. In this paper, we propose a scheme called *Modified Bloom's Scheme* (MBS) that uses asymmetric matrices of keys in place of symmetric matrices in order to establish secret keys between node pairs. The network resilience against node capture attack is improved using the proposed scheme.

Keywords - *Asymmetric Matrices, Key predistribution, Network Connectivity, Network Resilience, Node Capture Effect, Wireless Sensor Networks.*

I. INTRODUCTION

Wireless Sensor Networks[WSNs] are widely deployed at high density regions where surveillance and monitoring is required. WSNs find wide applications in the field of military especially in the process of sensing and tracking the objects and traffic signaling. WSNs are vulnerable to various kinds of attacks like eavesdropping, traffic analysis and masquerading. The nodes in the network forward packets on behalf of each other to the desired destinations. Security services like authentication and confidentiality are the critical issues to achieve secure communication between sensors in hostile environments. Traditional key management techniques using public key infrastructure or centralized key management techniques may not be suitable for sensor networks, since each node has constrained resources and they can be captured. Secret key pre-distribution for symmetric encryption is one of the practical approaches for establishing secure links between the sensor nodes.

Key Management includes the problem of *Key Distribution*. The three types of key distribution schemes are the trusted server scheme, the self-enforcing scheme and the key predistribution scheme. The *trusted server* scheme depends on a server that is having trustworthiness for key distribution between the nodes. The *self-enforcing* scheme is based on the concept of asymmetric cryptography. Using public key algorithm is not viable for sensor nodes, since there is a limitation on computation and energy resources [1]. The third type of key agreement scheme is key pre-distribution, in which the key information is distributed among all sensor nodes prior to deployment by knowing which nodes are more likely to be the same neighbors before deployment.

A number of key pre-distribution schemes exists in the field of sensor networks. One of the researcher propose that all the nodes carry a master secret key which is stored in a tamper resistant hardware. This reduces the risk, but increases the cost and energy consumption of each sensor [2]. If one node is compromised then the security of entire sensor network is compromised. So achieving network resilience becomes difficult. The performance of the Key Management Schemes can be evaluated based on the connectivity, resilience to sensor node capture, scalability and memory efficiency. Resilience of a node is the fractional amount of keys information exposed adversely so that the information can be retrieved [3]. Some of the network layer attacks in WSNs includes node capture attacks, selective forwarding, sinkhole attacks, sybil attacks, wormhole attack, spoofed attack, HELLO flood attacks and acknowledgment spoofing. Connectivity is determined based on the probability that atleast one common key is shared between any two nodes at a given time must be greater when smaller number of keys are used.

Motivation: Du *et al*.,[4] have proposed a key predistribution scheme which makes use of the deployment knowledge in order to increase the connectivity and resilience of the network. It is observed that in *Bloom's Scheme* the key predistribution scheme uses symmetric matrices in order to establish secret keys. It results in the establishment of a single key for communication between two sensor nodes. If this single secret key is captured by an adversary the communication between the node pair is permanently destroyed and the resilience of the network is reduced.

Contribution: *Modified Bloom's Scheme* is proposed in this paper which improves the resilience of the sensor network. In this scheme, *asymmetric matrices* are used instead of symmetric matrices which generates two secret keys to communicate between any two sensor nodes (say *n1*and *n2*). One key is used to communicate from node *n1* to *n2* and another to communicate from node *n2* to *n1* as shown in Figure 1. Two separate communication links are established between a pair of nodes. If one of the communication link gets compromised by an adversary, still another link exists to communicate between the nodes thus, increasing the resilience of the sensor network.

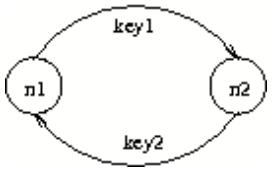

Figure 1. Example of generation of establish communication between any two nodes.

Organization: The paper is organized as follows. Literature Survey is discussed in Section II, Model and Problem Definition in Section III. Section IV includes Implementation and Section V discusses the Simulation and Performance Evaluation. Conclusion is presented in Section VI.

II. LITERATURE SURVEY

Dong et al., [3] investigated that the key predistribution scheme are classified as (i) Pure Probabilistic Key Predistribution, (ii) Polynomial based Key Predistribution, (iii) Bloom's Matrix based Key Predistribution and (iv) Deterministic Key Predistribution Scheme. It is observed that in order to improve the performance of Key Management Schemes like resilience against node capture, connectivity and memory efficiency, it is better to use location based knowledge. Eschenauer et al., [4] proposed a Random Key Pre-distribution Scheme in which each sensor node receives a random subset of keys from a large key pool before deployment. Two nodes find one common key within their subset and use this key as their shared secret key. Bloom et al., proposed a key predistribution method that allows any pair of nodes in a network to derive a pairwise secret key [5]. All communication links of nodes that are noncompromised are secure and is referred to as λ-secure until more than λ nodes are compromised.

Chuang et al., [6] proposed a Scalable Grouping Random Key Pre-distribution Scheme which divides all nodes into several groups. To improve resilience against node capture, they have considered the link key to be composed of some shared keys. Leonardo et al., [7] developed a scheme to setup keys for securing node to cluster-head communication called Secure Low Energy Adaptive Clustering Hierarchy [8], using *Random Key Pre-distribution*. Tran et al., [9] presented a new pairwise key predistribution scheme for sensor networks. This scheme utilizes merits of the two existing key pre-distribution schemes- *LU Key Decomposition Scheme* [10] and *Bloom's Symmetric Key Generation Scheme* with some modifications. Seyit et al., [11] presented a novel, deterministic and hybrid approaches based on combinatorial design for deciding how many and which keys to assign to each key chain before the deployment of sensor networks.

Du et al., proposed a new key predistribution scheme, which substantially improves the resilience of the network and better threshold property in [12] and an Improved Key Pre-distribution Scheme using multiple key spaces called DDHV Scheme in [13]. The DDHV scheme first constructs ω key spaces using Bloom's Scheme and then each sensor node carries key information from randomly selected key spaces τ (with $2 \leq \tau < \omega$). It is no longer certain that two nodes generates a pairwise key. In [14] Du et al., proposed a new key pre-distribution scheme which makes use of such a deployment knowledge called DDHV-D scheme. It is a modification of DDHV scheme [12]. Deployment knowledge in DDHV-D scheme is modeled using probability density functions. For example, let us consider the case where sensors are deployed by being dropped by an helicopter. The *Deployment point* is location of the helicopter and resident point is the point where the sensor actually resides. If we know perfectly the neighbors of each node in the network, key pre-distribution becomes trivial: For each node n_i, we just need to generate a pairwise key between n_i and each of its neighboring nodes

and save these keys in n_i's memory. This guarantees each node to establish a secure link with each of its neighbors after deployment.

Stinson et al., [15] analyzes and proves the Key Redistribution Techniques proposed by Cichon, Golebiewslu and Kutylowsk. They use long term keys to encrypt temporal keys that a base station broadcasts to the network and the temporal keys are used as session keys by the nodes in the sensor networks. Kousalya et al., [16] proposes a Traffic-Aware Key Management Scheme for WSNs based on the topological information of the network. They establish shared keys for active sensor nodes which participate in direct communication without disturbing the ongoing security process. Thus, increases the resilience, reduces energy consumption and increases the delivery ratio. Tague et al., [17] presents that the adversary corrupts the network and takes control over the nodes in the network by considering the passive attacks, active attacks and physical attacks together called as *node capture attack*. The adversary may replicate or corrupt the information in the nodes, thus leading to malfunctioning of the network.

Farshid et al. [18] have proposed a Hypercube Multivariate Scheme (HMS) in which they design a multidimensional hypercube grid such that each point on the grid is at the intersection of some multivariate polynomials. Using this scheme, every two sensor nodes at the hamming distance of one from each other are able to establish a direct key. Based on the HMS scheme, the authors have also designed a location-aware key predistribution scheme called hexagonal key predistribution. In this scheme, the target field is divided into overlapping hexagonal cells that provide an efficient coverage of the deployment field. The HMS scheme is used to predistribute keys in every cell. Shaila et al., proposed the Modified Blooms Scheme in which asymmetric matrices is used for the Key Predistribution and this paper is the extension of the work in [19].

III. Model And Problem Definition

A. System Model

The sensor nodes in the WSNs are considered to be static after deployment. The sensor nodes that are desired to be deployed in a particular location, this location is called as *Deployment points*. In the actual scenario, the sensor nodes reside around these deployment points based on certain probability density function and these points are called as *resident points*. The density function is a part of $G_{i,j}$ and are nonuniformly distributed. The distance between resident point and deployment point is less than 3σ with probability of 0.9987 as in [15]. The sensors are deployed using two dimensional Gaussian distribution. When the deployment point of group $G_{i,j}$ is at (x_i,y_j), then $\mu=(x_i,y_j)$ and the probability density function for node k in group $G_{i,j}$ is,

$$f(x,y|k \in G_{ij}) = \frac{1}{2\pi\sigma^2} e^{\frac{-[(x-x_i)^2+(y-y_j)^2]}{2\sigma^2}}$$

B. Problem Definition

Given a Wireless Sensor Network consisting of N number of nodes, which are divided into $t*n$ groups $G_{i,j}$ (for $i=1,...,t$ and $j=1,...,n$), a global key space pool S is also divided into $t*n$ groups $S_{i,j}$ (for $i=1,...,t$ *and* $j=1,...,n$) consisting of ω key-spaces and deployed over an area of X x Y using the above described deployment model. The problem is to predistribute τ key-spaces from ω key-spaces present in the key-space pool S to each node of each group and then calculate the secret key so that the resilience of the network is increased.

TABLE 1
Notations

Symbols	*Definition*
N	Network Size
S	Global Key-Pool Space
$\|S\|$	Size of global Key-space pool S
ω	Total number of key spaces
τ	Number of key-spaces put into each node
λ	Nodes that are compromised
σ	Standard Deviation of *Gaussian distribution*
R	Wireless Communication range for each node
R_c	The Attack Radius
a, b	The overlapping factors in key-space pool setup
$G_{i,j}$	$Tx n$ groups into which N network is divided
$S_{i,j}$	$Tx n$ groups into which global key-space pool S is divided
$K_{i,j}$	Secret key for communication from node i to node j
$K_{j,i}$	Secret key for communication from node j *to node* i

C. Assumptions

(i) The sensor nodes in the network are static after deployment.
(ii) The nodes are deployed *i.e.*, in a grid fashion with each node consisting of λ key spaces based on the Group Deployment Model.
(iii) Sensor nodes are equally divided into t x n groups G_{ij} for $i = 1, 2, \ldots, t$ and $j = 1, 2, \ldots, n$.
(iv) Global key-space is S with size $|S|$.
(v) The transmitting range of each node is assumed to be 50 meters.

IV. THE KEY PREDISTRIBUTION SCHEME

Modified Bloom's Scheme is aimed at allowing the sensor nodes to find a secret key with each of its neighbors after deployment. It consists of three phases:
(i) Key pre-distribution phase
(ii) Shared-key discovery phase
(iii) Path-key establishment phase
The first and third phase is exactly similar to the DDHV-D scheme [15], the second phase differs since the Modified Bloom's Scheme is used for the key generation.

Phase 1: Key Pre-distribution

Key pre-distribution phase is performed before the sensors are deployed in the area under surveillance. As in DDHV-D scheme, the key-space pool S is divided into t x n key-space pools $S_{i,j}$ (for i=1, . . . , t *and* j=1, . . . , n), with $S_{i,j}$ corresponding to the deployment group $G_{i,j}$. If the deployment groups are deployed in neighboring locations then the two key-space pools forms a neighbor. After setting the key-space pools, for each sensor node in the deployment group $G_{i,j}$, a random set of λ key-spaces is selected from its key-space pool $S_{i,j}$.

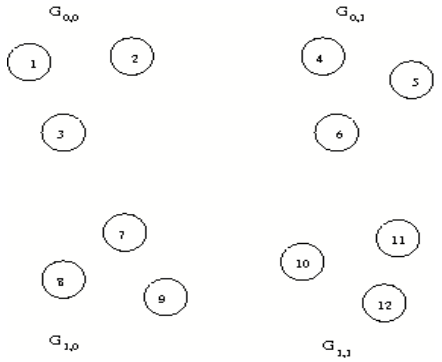

Figure 2. Sensor Network before execution of the three phases of *Key Predistribution Scheme*

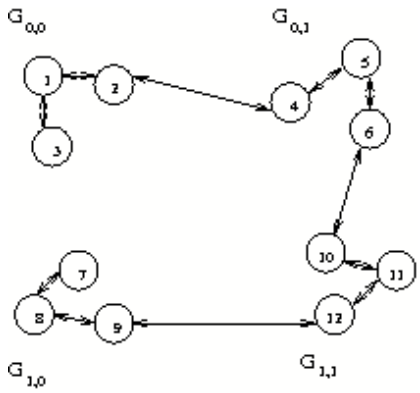

Figure 3. Sensor Network during the execution of the three phases of *KeyPre-distribution Scheme*

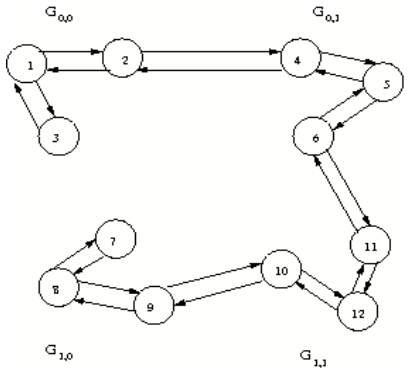

Figure 4. Sensor Network after the execution of the three phases of *Key Predistribution Scheme*

Phase 2:Shared-Key Discovery

This phase differs from the DDHV-D scheme since *Modified Bloom's Scheme* is used instead of the original Bloom's scheme. After deployment, each node tries to find whether it is sharing any key space with its neighbors. Broadcast a message from each node containing the indices of the key spaces it carries. Each neighboring node finds out if there exists a common key space that is shared with the broadcasting node. If such a key space exists, using the *Modified Bloom Scheme*, the two neighboring nodes derives a pairwise key from the common key space and use those keys to secure the communication links between themselves.

Modified Bloom's Scheme(MBS)

In this paper, a scheme used to establish secret keys between two nodes which shares the key spaces with each other is presented. This scheme is a modification of DDHV-D scheme and the original Bloom's Scheme. So, it is called as the Modified Bloom's Scheme (MBS). In MBS, assume some agreed upon $(\lambda + 1)$ x N matrix, G, over a finite field $GF(q)$, where, N is the size of the network and $q < N$. This matrix G is public information and may be shared by different systems, even the adversaries are assumed to know G. During the key generation phase, the base station creates a random $(\lambda$ x $1)$ x $(\lambda$ x $1)$ asymmetric matrix instead of the symmetric matrix D over $GF(q)$ generated in the original Bloom's scheme and computes an N x $(\lambda + 1)$ matrix $A = (D.G)^T$. Matrix D should be kept secret and should not be disclosed to adversaries or to any sensor nodes. Since, D is not a symmetric matrix A . G is also not a symmetric matrix. Suppose $K = A.G$, then the result is $K_{i,j} \neq K_{j,i}$, where $K_{i,j}$ and $K_{j,i}$ are the elements in the i^{th} row and j^{th} column and j^{th} row and i^{th} column of K respectively. To carry out the above computation, nodes i and j should be able to compute $K_{i,j}$ and $K_{j,i}$ respectively. This can be easily achieved by modifying the Bloom's Scheme. The idea is to use key $K_{i,j}$ to secure the communication link from node i to node j and key $K_{j,i}$ to secure the communication link from node j to node i. There exists bi-directional links between each pair of nodes which share the key-spaces.

Phase 3:Path Key Establishment

There is a possibility that two neighboring nodes cannot find any common key space between them. In this case, they need to find a secure path to agree upon a common key. It can be observed that two neighboring nodes, i and j, do not share a common key space; but still come up with a secret key between them. The idea is to use the secure links that have already been established in the key-space sharing graph.

Global Key Space (GKS): As long as the graph is connected, two neighboring nodes i and j can always find a path in *GKS* from i to j. Assume that the path is $i, v_1, \ldots, v_h, j$. To find a common secret key between i and j, i first generates a random key K. Then, i sends the key to v_1 using the secure link between i and v_1 ; v_1 forwards the key to v_2 using the secure link between v_1 and v_2 and so on until j receives the key from v_h . Nodes i and j use this secret key K as their pairwise key.

V. IMPLEMENTATION

In this paper, in order to analyze the *resilience* of the proposed scheme, an attack model is used for the adversaries attacks. The attack model assumes that:

(i) the adversary captures nodes randomly within the region of surveillance.

(ii) The region is assumed to be a circle centered at point with co-ordinate (x, y) with radius R_c, called the *attack radius* and the circle is termed as *attack circle*. When the circle is large enough to contain the entire deployment region, the attack model reduces to uniform-random attack, in which the probability that any node in the entire deployment region compromised is the same.

The effect of the capture of x_c sensor nodes in a node capture attack model by an adversary on the security of the remaining part of the network has is determined. *For example*: In Key pre-distribution phase, a 200*m* x 200*m* deployment area is considered. The area is then divided into a grid of size 4 = 2 x 2 = *t* x *n* with each grid cell of size 4*m* x 4*m*, so that the network is divided into four groups $G_{i,j}$, for $i = 0, 1$ and $j = 0, 1$ and each group consists of three nodes as shown in Figure 2.

Next, consider a global key-space pool of size 200 *i.e*., 200 key-spaces are present in the global key-space pool. The global key-space pool is also divided into $S_{i,j}$ groups, for $i = 0, 1$ and $j = 0, 1$. After the key-space pools are setup, for each sensor node in the deployment group $G_{i,j}$, are randomly selected from τ key-spaces from its corresponding key-space pool $S_{i,j}$. Then for each selected key space, load the corresponding row of its *A* matrix which is constructed using the MBS scheme into the memory of the node.

Next, in the shared key discovery phase, the nodes which share any key-spaces with its neighbors is discovered with the help of broadcasting messages. If such a key-space exists, using the MBS scheme, the two neighboring nodes derive secret keys and use these keys to secure the communication links between them. After this, construct a key space sharing graph which is already defined. Finally, in the path-key establishment phase flooding is used to establish secret keys between nodes which do not share any common key-spaces with each other as shown in Figure 3 and Figure 4. The network after the three phases looks like the one depicted in the Figure 5. Hence, there exists two communication links between each node pairs which share a common key-space.

To analyze the resilience of our scheme an *attack circle* of some randomly chosen radius is drawn at some randomly chosen point within the sensor network as shown in the Figure 6. Observe that the nodes which come under the attack circle are captured by the adversary as shown in Figure 6. The captured nodes are highlighted in Figure 7. In this example the nodes that come under the attack circle *i.e*., the nodes which are captured by the adversary are the nodes numbered 6, 10, 11 and 12. After the adversary captures these nodes, it is assumed that the communication links of these nodes are also compromised. Unlike in DDHV-D scheme, if node *i* is captured and it shares a common key space with node *j*, the bi-directional communication link between nodes *i* and *j* are not compromised completely. Instead, only the link from node *i* to node *j* is compromised but the link from node *j* to node *i* is still safe and out of adversaries reach since two different keys $K_{i,j}$ and $K_{j,i}$ are used to communicate from node *i* to node *j* and from node *j* to node *i* respectively. This can be made clear from the network scenario depicted in Figure 10. Here all the links that are present between node pairs (6,11), (11,12) and (10,12) are captured completely since these nodes come under the attack circle whereas the links between node pairs (6,5) and (10,9) are compromised partially(shown in dotted lines) *i.e.*, the link from node 6 to node 5 and the link from node 10 to node 9 are only compromised but the link from node 5 to node 6 and the link from node 9 to node 10 are safe. Because of this property, the resilience of the proposed key pre-distribution scheme is increased.

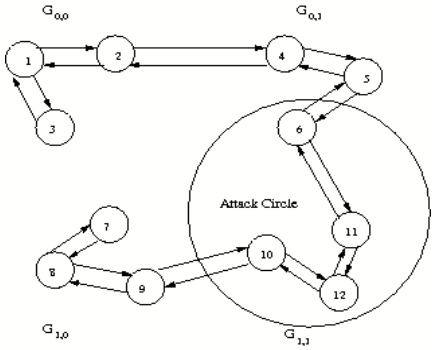

Figure 5. Sensor Network after the adversary attack depicting the *Attack Circle*

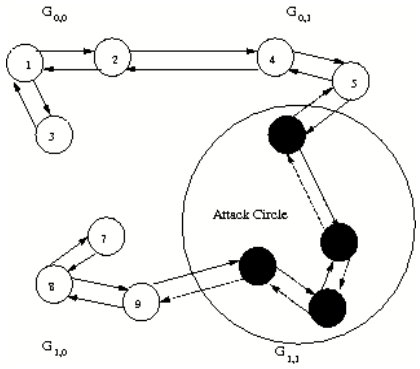

Figure 6. Sensor Network with the captured nodes highlighted

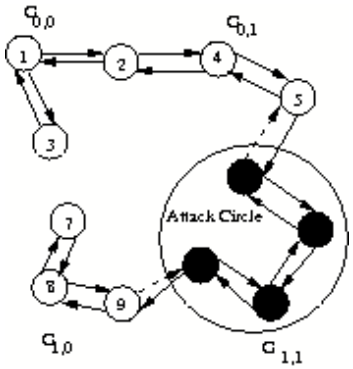

Figure 7. Sensor Network showing the destroyed or compromised links

VI. SIMULATION AND PERFORMANCE EVALUATION

A. Simulation Setup

The proposed scheme was simulated using NS2 simulator in the Fedora Core 6 platform to evaluate the performance of the proposed scheme. The results are also compared with the existing scheme. Different size of deployment areas were considered, since the simulation was performed on different network sizes. As per our assumption the node deployment follow a two-dimensional Gaussian distribution and the sensor nodes are static once they are deployed. The value of overlapping factors *a* and *b* were taken as 0.15 and 0.10 respectively and standard deviation , $\sigma = 25$. The wireless communication range for each node is taken to be $R = 40m$. The radius of the attack circle R_c was chosen randomly and the point at which the circle originates is chosen randomly.

B. Performance Evaluation

Resilience is a set of secure links that compromises when a certain number of nodes are captured by the adversaries. Assume that an adversary can mount a physical attack on a sensor node after it is deployed and secret information can be read from its memory. The aim is to find how a successful attack on *x* sensor nodes by an adversary affects the rest of the network. In particular, the number of communication links that an adversary can compromise is to be determined based on the information retrieved from *x* captured nodes.

Figure 8, Figure 9 and Figure 10 shows the simulation results on the resilience performance of MBS Scheme against node compromise. The performance metric is the number of communication links that are compromised when *x* nodes are captured. The MBS Scheme and the DDHV-D Scheme plot is shown in Figure 8. The simulation is run for a network of size $N = 200$ nodes and the graph is plotted to show the number of communication links that are compromised for different attack radius R_c. The graph shows that the communication compromise is reduced by 50% using MBS Scheme compared with the DDH-V Scheme. In order to study the resilience against node capture for varying network sizes, the simulation is run by keeping the attack radius constant. The results of these simulations are plotted as shown in Figure 9. The resilience of our scheme is affected by the attack radius R_c. When compromised nodes are more concentrated (*i.e.*, when R_c is smaller), the damage to the communication links is more severe, still the number of links compromising with increase in the network size is minimized compared to the existing scheme.

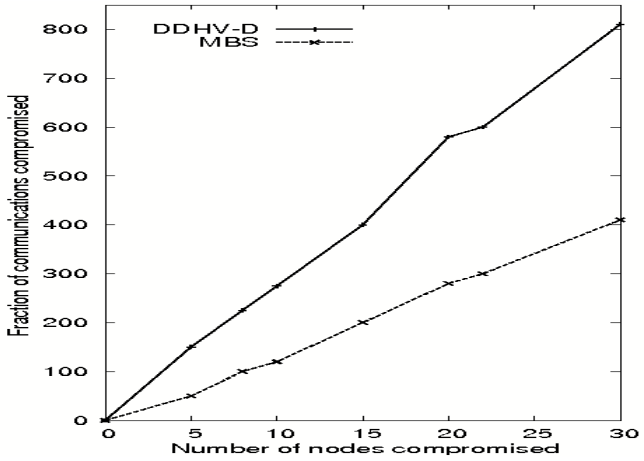

Figure 8. Resilience Analysis: The number of links compromised for a network

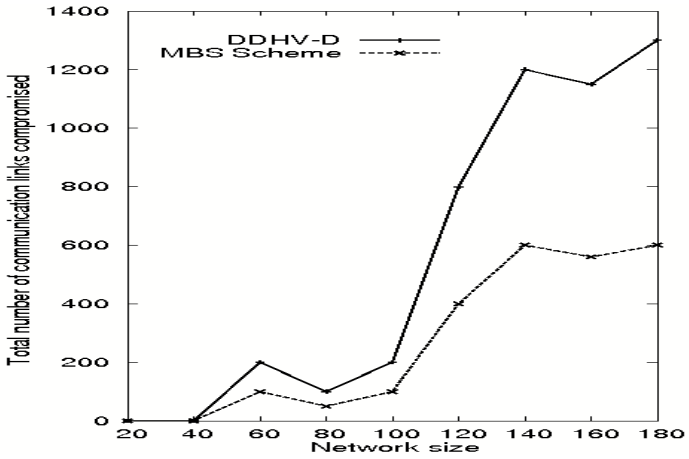

Figure 9. Resilience Analysis: The number of links compromised for different network sizes with constant attack radius R_c=25.

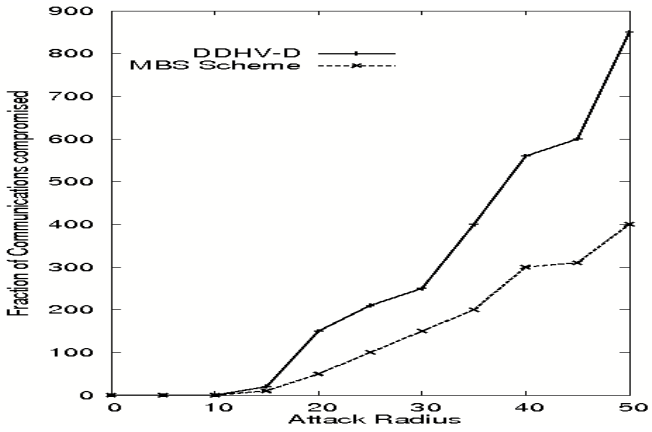

Figure 10. Resilience Analysis: The number of links compromised for a network of size N=200 with varying attack radius.

The plot in Figure 10 shows the resilience results for a number of different values of attack radius R_c. It shows that resilience becomes better when the compromised nodes are less concentrated. The compromise of the communication is reduced approximately by 60% for a fixed sized network consisting of 200 nodes and by varying the attack circle. This result is easy to understand, as the value of R_c increases, the compromised nodes become more and more evenly distributed among the deployment groups. Therefore, given the same x value (the

number of compromised nodes), the number of compromised nodes for each particular deployment group is less for a larger R_c than that for a smaller R_c.

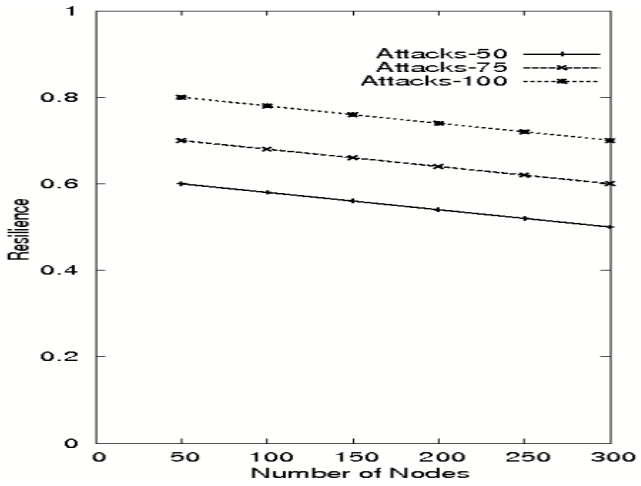

Figure 11. Resilience Vs Number of Nodes

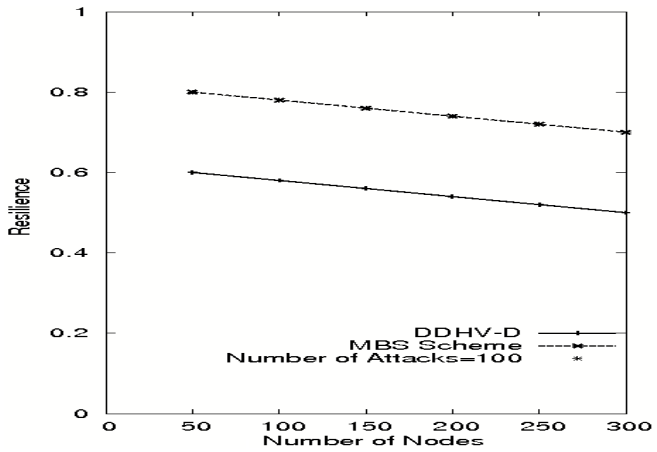

Figure 12. Resilience Vs. Number of Nodes with number of attacks=100

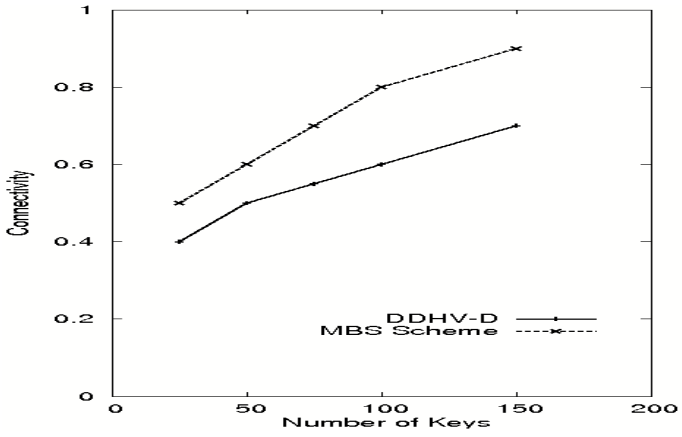

Fig. 13. Connectivity Vs. Number of Keys

Figure 11 illustrates that as the number of nodes is increased and with the number of attackers increased, the resilience of the network decreases. The graph illustrates that the Resilience of the network decreases gradually as the number of nodes increases for different attacks. The resilience increases with the increase in the number of nodes by 20% assuming constant attack value of 100 as shown in Figure 12. Figure 13 indicates that smaller

number of keys can be used to achieve the desired connectivity in each sensor. The energy consumption is reduced with increase in the number of nodes and by varying the attackers as shown in Figure 14. From graph it shows that the energy consumed by MBS Scheme is reduced by 20% compared with the DDHV-D Scheme.

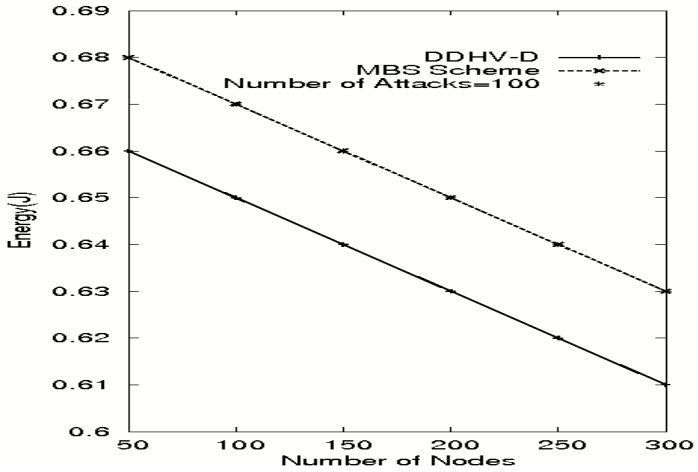

Figure 14. Energy Consumption Vs. Number of Nodes

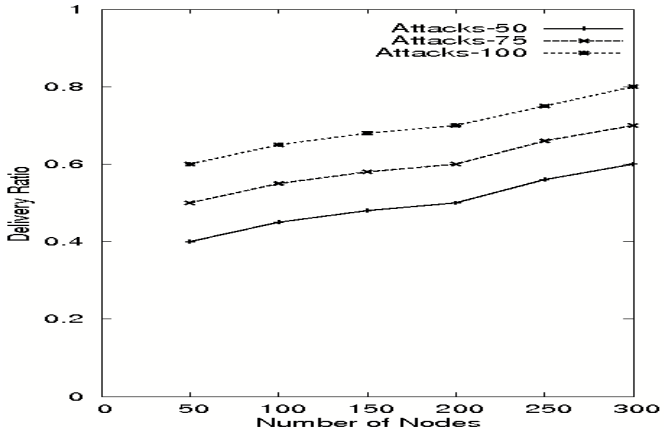

Figure 15. Delivery Ratio Vs. Number of Nodes

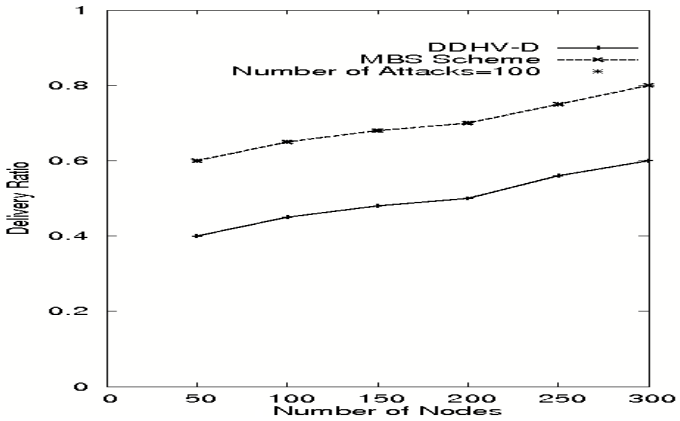

Figure 16. Delivery Ratio Vs. Number of Nodes with Number of Attacks=100

The paths are efficiently established and the data packets are transmitted, thus increasing the delivery ratio even though there is an increase in the number of attacks as shown in Figure 15. When compared with the existing scheme there is a drastic increase in the delivery ratio of data packets in MBS Scheme for any fixed number of attacks values as shown in Figure 15 and Figure 16.

VII. CONCLUSIONS

The *Modified Bloom's Scheme* (MBS) is more advantageous over the existing schemes since it decrease the number of communication links that get compromised. The secret keys between node pairs are derived such that they share a common key-space with each other. Unlike, in earlier schemes, two different keys are used to communicate between a pair of nodes. The simulation results show that the performance of MBS is better than the existing schemes in both the resilience against node capture effect and connectivity of the network. The resilience of the network increases with the increase in the number of attacks or with increase in the number of keys. The simulation results also show that the energy consumption is minimized and efficient packet delivery is achieved with the increase in the number of nodes.

REFERENCES

[1] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks," *Proceedings Seventh AnnualACM/IEEE International Conference on Mobile Computing and Networking(MobiCom)*, pp. 189-199, July 2001.

[2] R. Anderson and M. Kuhn, "Tamper Resistance-A Cautionary Note," *Proceedings Second Usenix Workshop Electronic Commerce*, pp. 1-11, November 1996.

[3] SUN Dong Mei and HE Bing, "Review of Key Management Mechanisms in Wireless Sensor Networks," *Journal on ACTA Automatica Sinica*, vol. 32, no. 6, November 2006.

[4] L. Eschenauer and V. D. Gligor, "A Key Management Scheme for Distributed Sensor Networks," *Proceedings Ninth ACM Conference Computer and Communication Security*, pp. 41-47, 2002.

[5] R. Bloom, "An Optimal Class of Symmetric Key Generation Systems," *Advances in Cryptology: Proceedings of EUROCRYPT 84*, pp. 335-338, 1985.

[6] Po-Jen Chuang, Tun-Hao Chao, and Bo-Yi Li, "A Scalable Grouping Random Key Predistribution Scheme for Large Scale Sensor Networks," *Proceedings of the Third International Conference on Information Technology and Applications (ICITA05)*, 2005.

[7] Leonardo B. Oliveira Hao C. Wong, M. Bern Ricardo Dahab, and A. A. F. Loureiro, "SecLEACH A Random Key Distribution Solution for Securing Clustered Sensor Networks," *Fifth IEEE International Symposium on Network Computing and Applications (NCA'06)*, 2006.

[8] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy Efficient Communication Protocol for Wireless Microsensor Networks," *IEEE Hawaii International Conference on System Sciences*, pp 4-7, January 2000.

[9] Tran Thanh Dai, Cao Trong Hieu, and Choong Seon Hong, "A Resource-Optimal Key Pre-distribution Scheme for Secure Wireless Sensor Networks," *Supported by MIC and ITRC project*, pp. 1088-1097, 2006.

[10] S. Choi and H. Youn, "An Efficient Key Pre-distribution Scheme for Secure Distributed Sensor Networks," *EUC Workshop, LNCS 3823, International Federation for Information Processing(IFIP)*, 2005.

[11] Seyit A. Camtepe, and Bulent Yener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks," *IEEE/ACM Transactions on Networking*, vol. 15, no. 2, April 2007.

[12] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks," *Proceedings of 10th ACM Conference on Computer and Communication Security (CCS)*, pp. 42-51, 2003.

[13] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," *Proceedings of IEEE INFOCOM'04*, pp. 586-597, 2004.

[14] W.Du, J. Deng, Y. S. Han and P. K. Varshney, "A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 1, 2006.

[15] Douglas R Stinson and David R, "Comments on a Sensor Network Key Redistribution Technique of Cichon, Golebiewski and Kutylowski," *Cryptology ePrint Archive:Report, University of Waterloo*, 259, 2011.

[16] C Gnana Kousalya and G S Anandha Mala, "An Energy-Efficient and Resilient Traffic-Aware Key Management Scheme for Wireless Sensor Networks," *European Journal of Scientific Research*, vol. 50, no. 2, pp. 246-262, 2011.

[17] Patrick Tague, Mingyan Li and Radha Poovendran, "Mitigation of Control Channel Jamming under Node Capture Attacks," *IEEE Transactions on Mobile Computing*, vol. 8, no. 9, pp. 1221-1234, 2009.

[18] Farshid Delgosha and Faramarz Fekri, "Key Pre-distribution in Wireless Sensor Networks using Multivariate Polynomials," *Second Annual IEEE Communications Society Conference on Sensor and Adhoc Communications and Networks, IEEESECON 2005*, pp. 118-129, 2005.

[19] Shaila K, S H Manjula, Aruna R, Anupama, Venugopal K R and L M Patnaik, "Resilience Key Predistribution Scheme using Asymmetric Matrices for Wireless Sensor Networks," *2009 IEEE International Advance Computing Conference(IACC 2009)*, pp. 2024-2031, 2009.

Shaila K is an Associate Professor in the Department of Electronics and Communication Engineering at Vivekananda Institute of Technology, Bangalore, India. She obtained her B.E and M.E degrees in Electronics and Communication Engineering from Bangalore University, Bangalore. She is presently pursuing her Ph.D programme in the area of Wireless Sensor Networks in Bangalore University. Her research interest is in the area of Sensor Networks, Adhoc Networks and Image Processing.

S H Manjula received Bachelor of Engineering in Computer Science and Master of Engineering in Computer Science from University Visvesvaraya College of Engineering, Bangalore University, Bangalore and Ph.D from Dr. M G R University, Chennai. She is working as Associate Professor in the Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. Her research interest includes Wireless Sensor Networks, Data Mining and Semantic Web.

Thriveni J received Master of Engineering in Computer Science from University Visvesvaraya College of Engineering, Bangalore University, Bangalore and Ph.D from Dr. M G R University, Chennai. She is working as Associate Professor in the Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. Her research interest includes Adhoc and Wireless Sensor Networks.

Venugopal K R is currently the Principal, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bangalore. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored 31 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ and Digital Circuits and Systems *etc*.. During his three decades of service at UVCE he has over 250 research papers to his credit. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining.

L M Patnaik is a Vice Chancellor, Defense Institute of Advanced Technology, Pune, India. He was a Professor since 1986 with the Department of Computer Science and Automation, Indian Institute of Science, Bangalore. During the past 35 years of his service at the Institute he has over 700 research publications in refereed International Journals and refereed International Conference Proceedings. He is a Fellow of all the four leading Science and Engineering Academies in India; Fellow of the IEEE and the Academy of Science for the Developing World. He has received twenty national and international awards; notable among them is the IEEE Technical Achievement Award for his significant contributions to High Performance Computing and Soft Computing. His areas of research interest have been Parallel and Distributed Computing, Mobile Computing, CAD for VLSI circuits, Soft Computing and Computational Neuroscience.