International Journal of Computer Theory and Engineering, Vol.3, No.1, February, 2011
1793-8201

Validation Time and Dynamic Speed to Enhance Secure Communication Rate in Wireless Sensor Networks

Shaila K*, Vidya Yeri*, Arjun A V*, Venugopal K R*, L M Patnaik**

Abstract—**Wireless Sensor Networks consists of sensor nodes that are networked in a surveillance area. Security is considered as one of the vital issues in the area of sensor networks. This work proposes an efficient scheme that deals with the availability of a mobile node for secure communication and introduces session time within which the secured secret key remains valid. The analysis and simulation results show that the performance of the proposed scheme is better than the existing schemes.**

Index Terms—**EX-OR operation, Mobile Node, Secret Key Distribution, Validation Time, Wireless Sensor Networks.**

I. Introduction

Sensor network is a large collection of tiny devices to monitor and interact with specific area of interest. These tiny devices are called as sensor nodes. Each sensor node consists of the following units : *(i) Power Unit* : It supplies the necessary power to other subsystems, *(ii) Sensing Unit* : It includes analog sensor instrument and analog-to-digital converter which samples the data and delivers to the processing unit, *(iii) Processing Unit* : It controls the operation of the sensor by processing the sensed data and stores them temporarily for later transmission, *(iv) Mobile Unit* : It is responsible for controlling speed and direction of the sensor nodes.

Wireless Sensor Networks (WSN) is widely used in military applications such as military command, control systems, communications, computers, intelligence and surveillance systems. The rapid deployment, self organization and fault tolerance characteristics of sensor networks make them a very promising technique for military applications. Some military applications are force tracking, battlefield surveillance, targeting and battle damage assessment. They are deployed in chemical, biological, radiological and nuclear detection.

Some environmental applications of sensor networks include tracking the movement of species, i.e., habitat monitoring, monitoring environmental conditions that affect the livestock, irrigation, micro instrument for large-scale earth monitoring and planetary exploration. WSN find wide application in the commercial areas like inventory management, product quality monitoring and environmental control in office buildings.

In industry, control systems rely on sensors and actuators to monitor and interact with physical processes. In a typical industrial system, sensor devices first transmit information to a control device. An industrial control system allows automated, accurate and fast control of a monitored system that could not be achieved by human interaction.

Advances in information and communication technology *i.e.,* in the areas of Micro Electrical and Mechanical Systems (MEMS) has led to the introduction of tiny sensing devices. These sensing devices consume low power and has low production cost. They are ideal for embedding in an environment so as to monitor or interact with it.

Some futuristic WSN applications include medical implant communication services, where numerous sensors and actuators are implemented in the human body for various purposes such as continuous monitoring, artificial immune system creation and paralyzed muscle stimulation.

In many of the above applications, mobile nodes are extensively used. Mobile nodes themselves can move or may be placed on the mobile objects which move in the network. For example : In military applications, sensor nodes on the vehicle would interact with the stationary sensor nodes to guide the path so that it does not enter hostile environment. Mobile node itself can move and sense the area of fire and send the information to the stationary node. Sometimes monitoring the entire area with stationary nodes is not reliable, alternatively mobile nodes are used along with stationary nodes.

Motivation : Communication between any two nodes in the network is performed in the presence of secret key that is shared among them to maintain network security. In the presence of the mobile node *M*, secret key is shared between source *S* and the destination *D*. Since mobile node is continuously moving, it may not be available to establish the shared key between *S* and *D* all the time. Due to the randomness in node deployment, communication is expected to be high in the dense part of the network rather than in the sparse network. In dense area, node *M* is expected to be

Manuscript received on December 20, 2009.

Shaila K is a Research Scholar at University Visvesvaraya College of Engineering, Bangalore, Corresponding author, phone: +91-9964579958; e-mail: shailak17@gmail.com.

*Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore 560 001

** Vice Chancellor, Defence Institute of Advanced Technology (Deemed University), Pune, India

present for a longer duration than the usual time.

Contribution: To achieve secure communication, an efficient key distribution scheme is proposed. Based on the rate of communication, the mobility of the node *M* is varied. For dense part of the network, mobility of node *M* is decreased due to the possibility of high level of communication. The mobility of the node *M* is increased in the sparse part of the network since the request for key exchange during communication is low. In the network, communication is continued even if the mobile node is not in the communication range of communicating nodes. This is possible as the key shared between sensor nodes is valid and is secure for certain session time. Within the session time communication can be performed using the existing shared key in the absence of node *M*.

Organization : In Section II, various research works related to routing security technique and Key Management technique is explained. Section III states Problem definition. Model and Algorithm to provide adaptive mobility and availability of a mobile node for Secret Key Distribution is proposed in Section IV. Implementation and Performance evaluation details are explained in Section V. Simulation details is presented in Section VI. The conclusions of the paper is discussed in Section VII.

II. Literature Survey

Chris et al., [1] have considered the routing security in Wireless Sensor Networks. Many existing protocols concentrates on network routing but, none of them have considered security as a goal. In this work, two classes of attacks against Sensor Networks *i.e.,* sinkholes and HELLO floods are explained and cripping attacks against all of them are specified. The proposed algorithm suggests countermeasures for the explained attacks.

Wenliang Du et al., propose Key Management Scheme for Wireless Sensor Network in [2]. Many key agreement schemes used in general networks such as *Diffie-Hellman Key Exchange* and *Public Key Based Schemes* are not suitable for Wireless Sensor Networks. Pre-distribution of secret keys for all pairs of nodes is not viable, due to the large amount of memory used when the network size is large. Noticing that in practical scenarios, certain deployment knowledge is available apriori, a novel random key pre-distribution scheme is proposed which exploits deployment knowledge and avoids unnecessary key assignments.

Germano et al., [3] evaluate security mechanism in WSN. Building a security service remains a considerable challenge due to the resource constraints. This work evaluates the security mechanism on sensor node and the network as a whole. Measurement have shown that integrity code length added to application messages using cryptographic algorithms is acceptable for a sensor node with 128KB of ROM memory and 4KB of RAM. It is evaluated that power consumption for encryption technique does not cause representative impact on the network operation.

Noureddine et al., presents a new Key Distribution Scheme to improve the existing one which are not suitable for Wireless Sensor Network in [4]. This scheme makes use of coordinator sensor nodes, increasing the number of nodes that is to be captured by an adversary. This scheme shows significant improvement in security but still vulnerable when certain number of sensor nodes are captured.

Paulo F Oliveira et al., [5] presents Secret Key Distribution Scheme for large sensor network. In this work they argue that, it is not a probabilistic scheme i.e., any two nodes that can communicate securely with the probability one, using small number of prestored keys at the expense of a mobile node for bootstrapping. But messages are distributed throughout the network. Since, communication between two nodes is dependent on the availability of a mobile node, it may not be available to assist all the communications. Communication fails if mobile node is not present in the range of the communicating nodes.

W Du et al., [6] presents a Key Distribution Scheme, which improves the resilience of the network compared to the existing schemes. When the number of compromised nodes is less than the threshold, the probability that any nodes other than compromised nodes is affected is close to zero. This property lowers the initial payoff of smaller scale network breaching to an adversary. Shaila et al., [7] proposed a Predistribution Scheme using Asymmetric Matrices, which improves the resilience of the Wireless Sensor Network. The Modified Bloom's Scheme uses asymmetric matrices to establish secret keys between node pairs. Though the resilience against node capture is improved, two different keys are required to establish communication between two nodes.

D Malan et al., [8] proposed an elliptic curve cryptography. They argue that even though secret key cryptography has been used, there is a necessity for an efficient, secure mechanism for distribution of secret keys among nodes. Even though public-key infrastructure has been thought impractical, authors demonstrate that public keys can be generated within 34s using 1Kilobyte of SRAM and 34Kilobytes of ROM.

A Perrig et al., [9] presents security building blocks optimized for resource constrained environment. It has two secure building blocks SNEP and μ TESLA. SNEP provides the following important baseline security primitives: Data confidentiality, Data Authentication and Data Freshness. The problem is to provide efficient broadcast authentication, which is an important mechanism for sensor networks. μ TESLA is a new protocol suite which provides authenticated broadcast for severely resource constrained environments.

Debao Xiao et al., [10] present sensor protocol for information negotiation(SPIN). It is a data centric routing protocol of sensor networks. It is secure extension of SPIN protocol which is divided into three phases and use some cryptographic functions. This scheme increases the data communication security in the network. L Eschenauer et al., [11] proposed random key pre-distribution scheme that uses deployment knowledge in WSN. This scheme reduces the memory usage which relieves the memory requirement in memory constrained sensor node. It improves the network's resilience against node capture but

this scheme assumes the deployment knowledge which is not feasible in all the applications.

S Zhu et al., [12] explains localized encryption and authentication protocol. It is a key management protocol for sensor networks to support in-network processing. This protocol also restricts the security impact of a node compromise to the immediate network neighborhood of the compromised node. To support LEAP, four types of keys are used *(i)* An individual key shared with the base station. *(ii)* A pairwise key shared with other sensor node. *(iii)* A cluster key shared with multiple neighboring nodes and *(iv)* A group key that is shared by all the nodes in the network. This protocol is used for establishing and updating these keys in communication. It is energy efficient since it minimizes the involvement of the base station but suffers from computational overhead and huge memory requirement, since large number of keys are required for maintainance.

C Fragouli et al., [13] compares the concept of network coding approach with the traditional method. With this technique, there is throughput improvement and high degree of robustness. This work mainly concentrates regarding the benefits of network coding. K Bhattad et al., [14] proposed a secure data transmission on an acyclic multicast network. A new theoretic model for security is proposed which defines the system as secure if an eavesdropper is unable to get any meaningful information about the source. It considers the case when the number of independent messages available to the eavesdropper is less than the multicast capacity of the network.

One of the advantages of having mobile nodes in Wireless Sensor Network is explained in [15]. In traditional client/server based computing architecture, data at multiple sources are transferred to a destination; whereas in mobile node based scenario, a task specific executable code traverses the relevant sources to gather data. The mobile nodes greatly reduce the communication cost over low bandwidth link. This can be achieved by moving the processing function to the data rather than bringing the data to the central processor. Min Chen et al., [15] explains the MAWSN (Mobile Agent based Wireless Sensor Network) Scheme which shows better performance than client/server communication in terms of energy consumption and packet delivery ratio. But, it suffers from longer end-to-end latency than client server communication.

III. Problem Definition

Mobile node *M* is responsible for key distribution across the network. Keys exchanged between any two nodes in the presence of node *M* is considered as secured key. The main objectives of this work is to :

1) Increase the availability of mobile node to the sensors so as to establish secure communication.
2) Increase the communication rate between the sensors even when mobile node is not in its range.
3) Mobile node dynamically adapts its mobility depending on the number of source nodes in its vicinity.

Assumptions

1) Mobile nodes are required for bootstrapping.
2) Every source node tries to communicate with other destination nodes continuously.
   (i) All nodes are homogeneous except mobile node *M*.
   (ii) Mobile node cannot be malicious.

IV. Model And Algorithm

Sensor network is a collection of sensor nodes which communicate with each other to exchange information. There are some applications where information needs to be transferred securely. To achieve this, network coding approach is used as in paper [5].

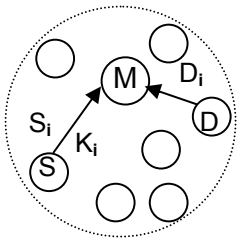

Fig. 1 Establishment of source, destination and key identifier when a source node sends the request message.

In this approach, network consists of *m* sensor nodes and one mobile node *M*. All the sensors have equal capacity interms of memory, battery and processing power. Compared with the normal nodes, node *M* has the following features:

1) *Large Memory*: Large memory is required to store all the keys that are present in the global key pool. Node *M* comprises of large memory since it has to establish a secure communication with each node in the network. It is achieved only when, there exists a shared key between every node with node *M*.
2) *Extra-energy*: Node *M* continuously moves throughout the network to establish secure communication between source and destination. Hence, it requires more energy when compared to static nodes *i.e.,* nodes with no mobility.
3) *Processing Power*: Node *M* is expected to have more processing power compared to other sensor nodes since, it has to assist the key exchange operation.

Before node deployment, each node is prestored with set of *k* local keys that are drawn from global key pool *G*. *G* is a pool of *n* keys from which *m* nodes access *k* keys such that, $mk \leq n$.

All local keys across the network are stored as global key pool in node *M*. Thus, global keys are not accessible by sensor nodes after deployment. All the nodes are randomly deployed in the area of interest. Node *M* continuously moves throughout the network and broadcasts *hello* message, to indicate the sensor nodes the presence of node *M*. When the nodes receive the *hello* packet from node *M*, it performs the following operations:

1) If a node is a source node, it wants to communicate with other nodes.
2) If a node is a destination node, all node wants to communicate with source node. But, each non-source node does not have the prior information about any node, that wants to communicate with it. So, all non-source

nodes are considered as destination nodes.

If the node which receives the *hello* message is a source node then it sends the communication *request* message which contains the following fields:

1) Source node identifier S_{id}.
2) Destination node identifier D_{id}.
3) Key identifier K_{id}, is an index of local key at each node.

Then, encrypt this message with the shared key between source node and node *M*.

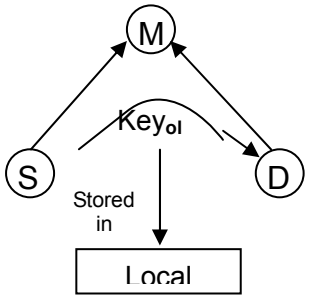

Fig.2 Before expiry of validation time.

If the received node is a destination node then it sends a *reply* message which contains K_{id} of destination for communication as shown in Figure 1. Again, this packet is encrypted with shared key between sensor node and the node *M*. On receiving the request from the source node, node *M* decrypts with the same session key and determines the D_{id} and K_{id} of a source node. Meanwhile, Node *M* also receives the *reply* message from the destination node. Node *M* retrieves both source and destination keys as S_{id} and D_{id} respectively from the global key pool present in node *M*. Node *M* then performs X-OR operation on both the keys S_k and D_k obtained from S_{id} and D_{id} as shown below,

$$key_{s,d} = S_k \oplus D_k$$

Then, $key_{s,d}$ is communicated to both *S* and *D*. At the source node, it performs the following operation and then retrieves the destination key,

$$D_k = key_{s,d} \oplus S_k$$

At the destination, source key is obtained by performing,

$$S_k = key_{s,d} \oplus D_k$$

In this way, keys are exchanged between nodes *S* and *D*. Once the keys are exchanged, then the key corresponding to each destination is stored in it's local table of a source node along with the validation time *t*. Similarly, key corresponding to source node is stored in the local table of a destination node. The *Validation time* represents the duration of time, until the key is valid. The node *M* sends the X-OR key results, to both the communicating nodes and moves further to assist other communication in the network to take place.

When there is a request for a communication from a source node, the node *M* has to cease it's mobility and then assist other sensor nodes in establishing the shared keys. Meanwhile, there are some nodes which are present in other parts of the network, which needs the assistance of node *M* in establishing the shared key. But, the node *M* not available to assist the transfer of information. Each source node has to wait for node *M* to come in the communication range. If the node *M* is not available, then secure communication is not possible. To achieve the secure communication, one solution is to use an existing key for a time duration *t*. Once the key is determined for each node, it is given a validation time until it is secure to use the existing key and this is stored in the local table. After the time expires, it is not secure to use the shared key. So, the communication that occurs before time *t*, makes it possible to use the key present in the local table.

During network operation when any source node wants to communicate with the destination node, one of the following conditions occur:

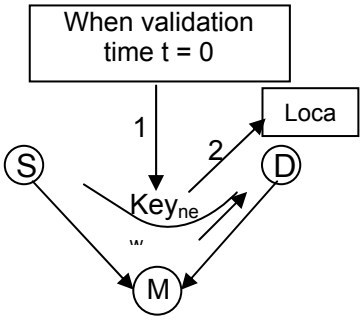

Fig. 3 After expiry of validation time. 1.When validation time t =0, a new key is generated, 2.The new key generated is stored in the local table again.

1) *Node M is available but key is not available* : For the first time when any node wants to communicate with the destination node, it utilizes the assistance of node *M* and establishes a session key. As shown in Figure 2 the session key, thus generated is stored in the local table as key_{old}.
2) *Both node M and key is available* : In this case node *M* is considered to be in the communication range and key validation time is not expired *i.e.*, validation time *t* which decrements with the elapse in time is not zero. The validation time *t* gets expired when its value reaches zero. Once, the validation time expires the key key_{old} is removed from the local table, since it is not secure to use the existing key from this point.

   In this situation, instead of using the existing key *i.e.*, key_{old}, utilize the assistance of node *M* to establish the shared key key_{new}. Figure 3 shows the generation of the new key when the validation time is zero and the new key is stored in the local table until the validity period expires. The key obtained from node *M* at this instance key_{new} is more secure than key stored in the local table key_{old} because, key_{new} is a recent one and no communication has been performed using this key and attacker cannot predict the value of the shared key.
3) *Node M is not available and* key_{old} *is available in the local table*: Since node *M* is busy in assisting other nodes in establishing the shared key, it is not available for current communication. Then, instead of waiting for node *M* to come in the communication range and provide shared key, it is possible to use the key present in the local key table key_{old} if the key is not expired.
4) *If both node M and* key_{old} *is not available*: In this condition, both means of communication are not available. Some nodes are able to establish the shared key with the destination. Thus, it leads to the failure of communication. The inference is node *M* is not available to source node for more than *t* time period. One of the reason is, it assists other communications or it is traversing through the area where there is no

communication.

If the node *M* is traversing through sparse communication then, node *M* need not have to spend much time in that area. Then, increase the speed *S* in that area, so that the area of sparse communication is traversed very fast. In the area where, high level of communication is required, node *M* has to spend more time so as to provide assistance to the source nodes. Hence, speed of node *M* is decreased in order to assist maximum number of communication of the messages.

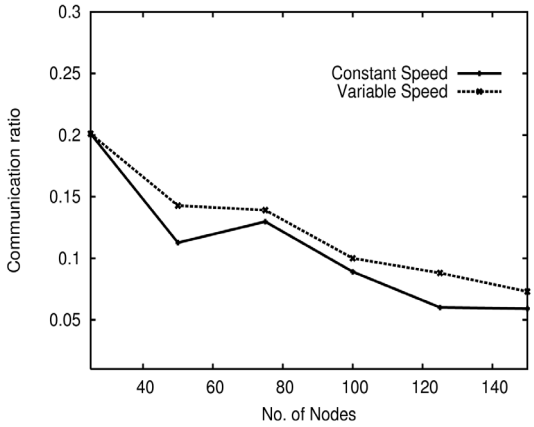

Fig. 4 Variable Speed Vs Constant Speed.

V. Implementation And Performance Evaluation

Proposed algorithm is implemented using NS2.31 Simulator in Fedora10. The surveillance area considered is 600m x 600m and the algorithm is evaluated for 25 to 150 nodes. There are several messages that have been used to evaluate the performance of the algorithm interms of secured communications between source node and destination node :

1) *Hello message* : Mobile node moves throughout the network continuously and broadcasts the *hello* message to indicate it's presence near the communicating nodes.
2) *Request message* : On receiving a *hello* message from a mobile node if the received node is a source node then a *request* message is sent to node *M* to establish the communication.
3) *Information message* : Sensor nodes receive a *hello* message from node *M*. If that particular node is not a source node then it sends the *Information* message along with the key identifier indicating it's possibility of being a receiving node or destination node.
4) *Key message*: After receiving *request* message from a source node, node *M* verifies whether it has received an *Information* message from destination node. If the key identifier key_{id} of the destination is present then node *M* fetches keys of source and destination node corresponding to key identifier, from global key pool. These two keys are further EX-ORed and then the result is multicasted to both source and destination node.

During the simulation, the node deployment is considered to be random and uniformly distributed in surveillance area. Single mobile node is present in a network to bootstrap all the sensor nodes and also to establish secure communication between the pair of source and destination node. The direction of the node *M* is randomly chosen using uniform variate to ensure that node *M* moves all over the network. The speed of the node *M* is varied in certain range so that it moves slowly in the dense part of the network and faster in the sparse part of the network.

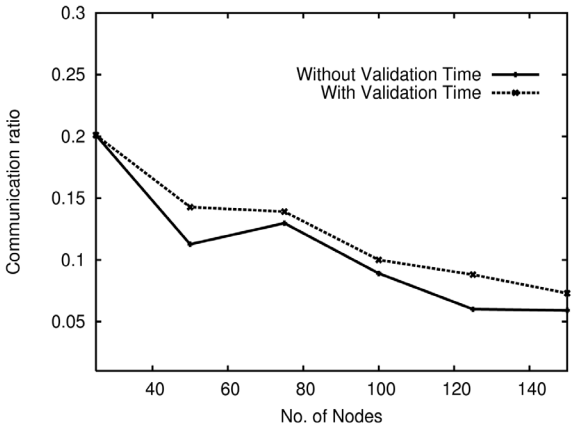

Fig. 5 No validation Time Vs With Validation Time.

In this algorithm, the validation time *t* is less than that of the *maximum time* taken by the adversary to hack the stored secret key for source-destination node pair. The maximum time refers to the time taken by an intruder to get into the network and give proxy either to the source or destination node. Every source node expires the validation time of key with a particular destination.

Since node *M* cannot be present always in the vicinity of every source node, the actual number of communication would always be less than that of the expected number of communication. Introducing the validation time increases the actual communication since node *M* is not mandatory for the communication to take place during the validation time.

The proposed scheme is analyzed by performing 30 simulations with different simulation time. Simulation result concentrates on communication ratio which is the total number of actual communication that took place to the number of expected communication to be taken place. Different communication ratios are obtained by varying the number of nodes.

In Figure 4, a graph of number of nodes versus communication ratio is plotted by considering the constant speed and variable speed as parameter. *Constant speed* is the concept in the existing scheme and *Variable speed* is based on the node density in the network as explained in the algorithm. From the graph, it is clear that communication ratio is considerably increased in the proposed scheme when compared to existing scheme.

In Figure 5, *Validation time* is considered as a parameter. During computation, if the destination key is not stored in the local table of a source node then, each time; the key computation is performed, when there is a request for communication. This scenario occurs when the validation time is not specified. The communication ratio obtained in this case is compared with the case when a validation time is specified for 15s.

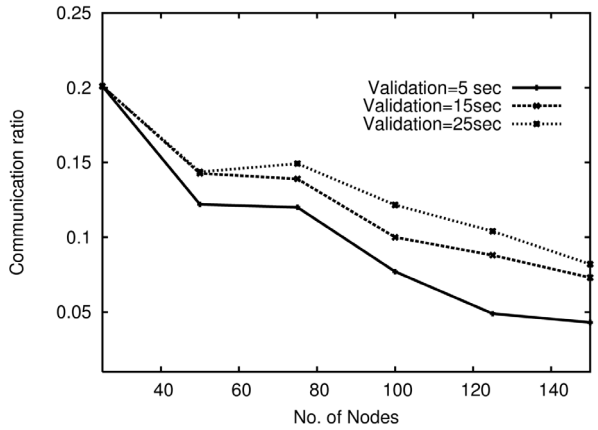

Fig. 6 Communication Ratio compared with different Validation Time.

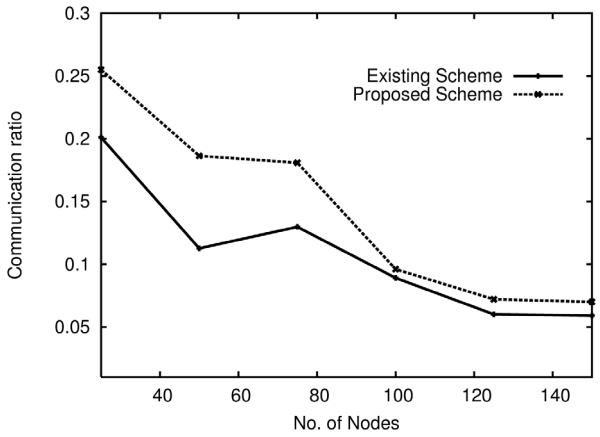

Fig. 7 Existing Scheme Vs Proposed Scheme.

Figure 6 shows the increase in communication ratio with increase in the number of nodes. The comparison between existing and proposed scheme is shown in Figure 7. In the proposed scheme:

1) Node *M* varies it's speed based on node density.
2) Computed key of a destination node is valid for time *t* which is not considered in the existing scheme. From the graph, it is clear that there is an increase in communication ratio when compared with the existing scheme and substantially more number of communication takes place when the number of nodes are less. Hence, it is inferred that the proposed scheme is well suited for small area with lesser number of nodes being deployed.

VI. Conclusions

The proposed scheme has several advantages over the existing scheme without affecting security in communication of the messages. The availability of a mobile node is increased dynamically by changing it's speed and the number of communications is increased by introducing the session time without affecting security. The simulation results show that the performance of proposed scheme has better performance than the existing scheme in both availability of a mobile node as well as in increasing the number of communication of the messages between the nodes.

References

[1] Chris Karlof and David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Counter Measurements," in Adhoc Networks, pp. 293-315, URL : http://www.elsevier.com/locate/adhoc, 2003.

[2] Wenliang Du, Jing Deng, Yunghsidng S Hant, Shigang Chen T and Prainod K Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," in Proceedings of the Twenty Third Annual Joint Conference of the IEEE Computer and Communications Socities, IEEE INFOCOM, vol. 1, pp. 586-597, March 2004.

[3] Germano Guimares, Eduardo Souto, Djamel Sadok, Judith Kelner, "Evaluation of Security Mechanisms in Wireless Sensor Networks," in Proceedings of the 2005 Systems Communications, IEEE Computer Society, USA, pp. 428-433, 2005.

[4] Noureddine Mehallegue, Emi Garcia and Gang Qu, "Improving Key Distribution for Wireless Sensor Networks," Second NASA/ESA Conference on Adaptive Hardware and Systems (AHS 2007), pp. 82-88, August 2007.

[5] P F Oliveira and J Barros, "A Network Coding Approach to Secret Key Distribution," IEEE Transaction on Information Forensics and Security, vol. 3, no. 3, pp. 414-423, September 2008.

[6] W Du, J Deng, Y S Han, P K Varshney, J Katz and A Khalili, "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks," ACM Transaction on Information Systems and Security., vol. 8, no. 2, pp. 228-258, 2005.

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

[8] D J Malan, M Welsh and M D Smith, "A Public-Key Infrastructure for Key Distribution in TinyOS based on Elliptic Curve Cryptography," Proceedings of the First International Conference on Sensor and Adhoc Communications and Networks, USA, IEEE Computer Society, SECON04., California, October 2004.

[9] A Perrig, R Szewczyk, J D Tygar, V Wen and D E Culler, "SPINS:Security Protocols for Sensor Networks,," in the Journal on Wireless Networks, vol. 8, no. 5, pp. 521-534, 2002.

[10] Debao Xiao, Meijuan Wei and Ying Zhou, "Secure-SPIN: Secure Sensor Protocol for Information via Negotiation for Wireless Sensor Networks," in Industrial Electronics and Applications, First IEEE Conference, pp. 24-26, May 2006.

[11] L Eschenauer and V D Gligor, "A Key-Management Scheme for Distributed Sensor Networks," in Proceedings of the Ninth ACM Conference on Computer and Communications Security, New York, pp. 41-47, 2002.

[12] S Zhu, S Setia and S Jajodia, "LEAP: Efcient Security Mechanisms for Large-Scale Distributed Sensor Networks," in Proceedings of the Tenth ACM Conference on Computer and Communications Security, New York, pp. 62-72, 2003.

[13] C Fragouli, J -Y L Boudec and J Widmer, "Network Coding: An Instant Primer," Proceedings SIGCOMM Computer Communications, vol. 36, no.1, pp. 63-68, 2006.

[14] K Bhattad and K Narayanan, "Weakly Secure Network Coding," Proceedings of the First Workshop on Network Coding, Theory and Applications, Riva del Garda, Italy 2005.

[15] Min Chen, Taekyoung Kwon, Yong Yuan and Victor C M Leung, "Mobile Agent Based Wireless Sensor Networks," Journal of Computers, vol. 1, no. 1, pp. 14-21, April 2006.

Shaila K is an Assistant 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 interests include Sensor Networks, Adhoc Networks and Image Processing.

Vidya Yeri is a Lecturer in the Department of Computer Science and Engineering at Alpha College of Engineering, Bangalore, India. She obtained her B.E and M.E degrees in Computer Science and Engineering from Bangalore University respectively. Her research interests is in the area of Wireless Sensor Networks.

Arjun A V is a Lecturer in the Department of Computer Science and Engineering at Alpha College of Engineering, Bangalore, India. He obtained his B.Tech and M.E degrees in Computer Science and Engineering from VTU and Bangalore University respectively. His research interests is in the area of Wireless Sensor Networks.

K R Venugopal 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 28 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ etc. He has been serving as the Professor and Chairman, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. During his three decades of service at UVCE he has over 200 research papers to his credit. His research interests include Computer 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 500 research publications in refereed International Journals and 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.