International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

Mitigate the Energy Consumption In Dynamic Wireless Sensor Networks Using Mathematical Model

K Rakesh
Assistant professor Department of Electronics and Communication Engineering
Joginpally BR Engineering College, Hyderabad, Telangana, India.

ABSTRACT:

Wireless sensor networks (WSNs) have been deployed for a wide type of packages, including navy sensing and monitoring, patient fame tracking, visitors float monitoring, where sensory gadgets regularly pass between exclusive places. Securing facts and communications requires appropriate encryption key protocols. In this paper, we use a certificates much less-effective key control (CL-EKM) protocol for at ease communication in dynamic WSNs characterised by means of node mobility. The CL-EKM helps efficient key updates when a node leaves or joins a cluster and guarantees forward and backward key secrecy. The protocol additionally supports efficient key revocation for compromised nodes and minimizes the effect of a node

compromise on the safety of other conversation hyperlinks. A safety evaluation of our scheme shows that our protocol is effective in defending in opposition to various attacks. In this paper, we layout mathematical model for mitigating the power intake. We put in force CL-EKM with mathematical technique using NS-2 simulator to assess its time, power, verbal exchange, and reminiscence overall performance.

INTRODUCTION:

DYNAMIC wireless sensor networks (WSNs), which enable mobility of sensor nodes, facilitate wider community coverage and more correct service than static WSNs. Therefore, dynamic WSNs are being unexpectedly adopted in tracking packages, inclusive of target tracking in battlefield surveillance, healthcare systems, site visitors float and automobile repute monitoring, dairy farm animals fitness monitoring. However, sensor gadgets are prone to malicious attacks such as impersonation, interception, seize or bodily destruction, due to their unattended operative environments and lapses of connectivity in wireless conversation. Thus, security is one of the most critical problems in lots of important dynamic WSN packages. Dynamic WSNs therefore want to address key safety requirements, inclusive of node authentication, records confidentiality and integrity, every time and anyplace the nodes circulate. On symmetric key encryption. Such

form of encryption is well-proper for sensor nodes due to their limited power and processing functionality. However, it suffers from excessive communique overhead and requires big reminiscence space to save shared pairwise keys. It is likewise no longer scalable and now not resilient against compromises, and not able to aid node mobility. Therefore symmetric key encryption is not suitable for dynamic WSNs. More lately, asymmetric key based strategies have been proposed for dynamic WSNs.

EXISTING SYSTEM:

In this paper, we use a Certificate much less Key Management scheme (CL-EKM) that helps the establishment of 4 types of keys, namely: a certificate much less public/private key pair, an individual key, a pair clever key, and a cluster key. This scheme additionally utilizes the principle algorithms of the CL-HSC scheme in deriving certificate less public/non-public keys and pair smart keys. We briefly describe the essential notations used in the paper (See Table I), the reason of these keys and the way they may be setup.

• **Certificate less Public/Private Key**: Before a node is deployed, the KGC at the BS generates a completely unique certificate much less non-public/public key pair and installs the keys in the node. This key pair is used to generate a jointly authenticated pair sensible key.

• **Individual Node Key**: Each node shares a unique man or woman key with BS. For example, a L-sensor can use the man or woman key to encrypt an alert message despatched to the BS, or if it fails to talk with the H-sensor.

An H-sensor can use its person key to encrypt the message corresponding to changes inside the cluster. The BS also can use this key to encrypt any touchy facts, including compromised node data or commands. Before a node is deployed, the BS assigns the node the
individual key.

• **Pair wise Key**: Each node shares a different pair smart key with every of its neighboring nodes for at ease communications and authentication of those nodes. For example, with a view to be part of a cluster, a L-sensor need to share a couple wise key with the H-sensor. Then, the H-sensor can securely encrypt and distribute its cluster key to the L-sensor by way of the usage of the pairwise key. In an aggregation supportive WSN, the L-sensor can use its pair clever key to safely transmit the sensed statistics to the H-sensor. Each node can dynamically establish the pair wise key between itself and some other node the use of their respective

certificates much less public/non-public key pairs.

• **Cluster Key:** All nodes in a cluster percentage a key, named as cluster key. The cluster secret's specifically used for securing broadcast messages in a cluster, e.G., touchy commands or the alternate of member status in a cluster. Only the cluster head can replace the cluster key when a L-sensor
leaves or joins the cluster.

DISADVANTAGES:

a)Key generation no longer in comfortable way

b)Energy stages less

c)Individual energy for node now not calculated

PROPOSED SYSTEM:

We propose a mathematical model for electricity intake. It approach that calculating the electricity for individual nodes and reduce the strength consumption for a secure way. Here the back down and keep values for node technology.

ADVANTAGES:

- Energy degrees are extra
- Individual node performance calculated
- Energy consumption less
- Secure extra

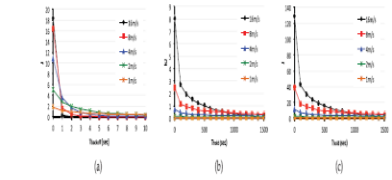


Fig. 8. Node movement simulation results in random walk mobility model. (a) Energy consumption of one H-sensor for cluster key update for one day (T_{hold} = 100 sec). (b) Energy consumption of one H-sensor for pairwise key establishment for one day ($T_{backoff}$ = 6 sec). (c) Energy consumption of one L-sensor for pairwise key establishment for one day ($T_{backoff}$ = 6 sec).

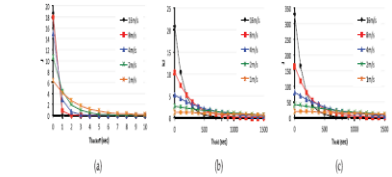
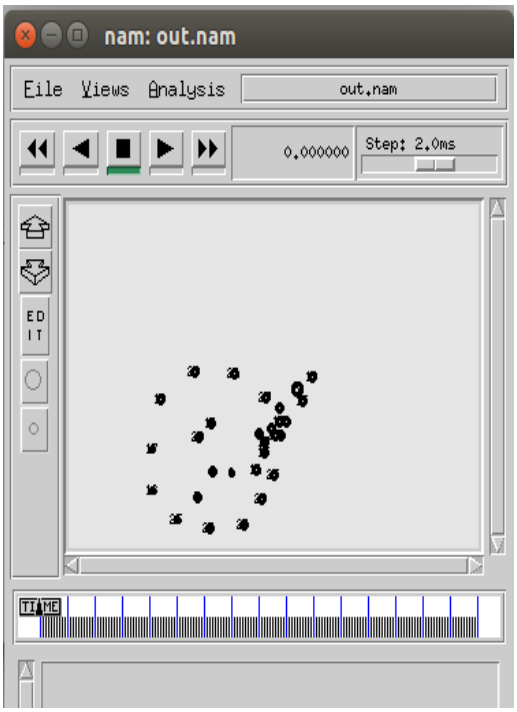


Fig. 9. Node movement simulation results in Manhattan mobility model. (a) Energy consumption of one H-sensor for cluster key update for one day (T_{hold} = 100 sec). (b) Energy consumption of one H-sensor for pairwise key establishment for one day ($T_{backoff}$ = 6 sec). (c) Energy consumption of one L-sensor for pairwise key establishment for one day ($T_{backoff}$ = 6 sec).

Effective key management dynamic WSNs



NAM WINDOW OUTPUT

CONCLUSION:

In this paper, we endorse the first certificates less effective key control protocol (CL-EKM) for secure conversation in dynamic WSNs. CL-EKM helps efficient conversation for key updates and control whilst a node leaves or joins a cluster and consequently guarantees ahead and backward key secrecy. Our scheme is resilient towards node compromise, cloning and impersonation assaults and protects the statistics confidentiality and integrity. The experimental outcomes reveal the efficiency of CL-EKM in useful resource confined WSNs. We recommend a mathematical model for power intake, based totally on CL-EKM with numerous parameters related to node actions. This mathematical model could be utilized to estimate the right cost for the Thold and Tbackof f parameters based totally on the velocity and the preferred tradeoff between the power consumption and the safety degree.

REFERENCES:

[1] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes

[2] for sensor networks," in *Proc. IEEE Symp. SP*, May 2003, pp. 197–213.

[3] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A key predistribution

[4] scheme for sensor networks using deployment knowledge," *IEEE Trans.*

[5] *Dependable Secure Comput.*, vol. 3, no. 1, pp. 62–77, Jan./Mar. 2006.

[6] W. Du, J. Deng, Y. S. Han, P. Varshney, J. Katz, and A. Khalili,

[7] "A pairwise key predistribution scheme for wireless sensor networks,"

[8] *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 2, pp. 228–258, 2005.

[9] M. Rahman and K. El-Khatib, "Private key agreement and secure communication for heterogeneous sensor networks," *J. Parallel Distrib.Comput.*, vol. 70, no. 8, pp. 858–870, 2010.

[10] M. R. Alagheband and M. R. Aref, "Dynamic and secure key management model for hierarchical heterogeneous sensor networks," *IET Inf.Secur.*, vol. 6, no. 4, pp. 271–280, Dec. 2012.

[11] D. S. Sanchez and H. Baldus, "A deterministic pairwise key predistribution scheme for mobile sensor networks," in *Proc. 1st Int. Conf.SecureComm*, Sep. 2005, pp. 277–288.

Author Profile:

Sri.Kolluri Rakesh, currently working as an Assistant Professor, in the

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

Department of Electronics and communication Engineering, Joginpally B.R Engineering college, Moinabad, Rangareddy Dist, Hyderabad, Telangana, India. He studied B.TECH (ECE) from J.B.R.E.C, JNTU University, Hyderabad and M.Tech(WIRELESS MOBILE COMMUNICATION) from, AHTC JNTU University, Hyderabad, India. He is having 1+ years of work experience in Academics, Teaching..