

## IMPLEMENTATION OF NOVEL PROTOCOL FOR KEY MANAGEMENT IN DYNAMIC WSN

M.Akhila Kumari<sup>1</sup>, Vishnu Prasad Goranthalala<sup>2</sup>

<sup>1</sup>M.Tech Student, <sup>2</sup>Associate Professor, Department of CSE, Balaji Institute of Engineering & science, Warangal District, Telangana, India.

**Abstract:** *Wireless device networks (WSNs) to replied continuous accessibility of the wireless medium to speak tributary the device nodes. Though, the open nature of this wireless medium leaves it exposed to multiple security threats or attacks. The secret writing key protocols square measure needed to securing information and communications. centrosymmetric key schemes square measure infeasible for mobile device nodes and thus past strategies have targeted solely on static WSNs. it's additionally not mountable and not sturdy compared to compromise nodes, and ineffectual to support node quality. thence centrosymmetric key's pertinent for dynamic WSNs. additional in recent times; uneven key primarily based strategies should be gift future for in dynamic WSNs. during this paper, a Certificate less Active Key Management (CL-AKM) protocol to supports key revocation in dynamic WSNs is projected. The projected theme is secure communication in dynamic WSNs and classified by node quality. Key updated once a node movement of node leaves or node connections a cluster and key revocation for compromised nodes square measure supported by our projected theme and ensures loco mote and backward key confidentiality. Our projected theme of security analysis is effective in an exceedingly variety of attacks. We tend to implement and simulate the Certificate less Active Key Management (CL-AKM) protocol exploitation NS2 machine to assess its energy, delay and threshold.*  
**Keywords:** *CL-AKM; Security; Key Management; AODV protocol; Node Mobility.*

### I. INTRODUCTION

A wireless device network (WSN) consists of an oversized range of device nodes, that area unit steam-powered by batteries, equipped with sensing, processing and short-range radio communication elements [1]. The applications of WSNs vary from the foremost common ones, like surroundings observance and residential automation, to a lot of stern ones in military or security areas, like field of honor police investigation, targeting and target pursuit systems. However, the wireless property, the shut interaction among device nodes and their unattended operation, similarly because the absence of physical protection create WSNs at risk of a good vary of network-level attacks and even physical harm [2]. despite the fact that device nodes will be equipped with integral tamper-resistance mechanisms, the memory chips area unit still affected by varied memory read-out vulnerabilities [3]. Key management may be a core mechanism to make sure security in network services and applications of WSNs. Key management will be outlined as a

group of processes and mechanisms that support key institution and therefore the maintenance of current keying relationships between valid parties in step with a security policy [4]. Since device nodes in WSNs have constraints in their machine power and memory capability, security solutions designed for wired and spontaneous networks aren't appropriate for WSNs. The goal of key management in WSNs is to resolve the matter of making, distributing and maintaining those secret keys. Hence, techniques for reliable distribution and management of those keys area unit of important importance for the protection in WSNs. because of their importance, the key management systems for WSNs have received increasing attention in scientific literature, and diverse key management schemes are planned for WSNs. reckoning on the flexibility to update the scientific discipline keys of device nodes throughout their run time (rekeying), these schemes will be classified into 2 totally different categories: static and dynamic. In static key management, the principle of key pre-distribution is adopted, and keys area unit fastened for the full life of the network. However, as a scientific discipline secret's used for a protracted time, its chance of being attacked will increase considerably. Instead, in dynamic key management, the scientific discipline keys area unit rested throughout the life of the network. Dynamic key management is thought to be a promising key management in device networks. Dynamic key management may be a set of processes accustomed perform rekeying either sporadically or on demand PRN by the network. Since the keys of compromised nodes area unit revoked within the rekeying method, dynamic key management schemes enhance network survivability and network resilience dramatically.

### II. RELATED WORK

According to the secure communication demand in WSN, 2 varieties of key institution are needed. One is pair wise key institution; the opposite is cluster key institution. A few schemes has been projected that incorporates 3 phases normally

- (1) key setup before deployment,
- (2) shared-key discovery once preparation, and
- (3) path-key institution if 2 sensor nodes don't share an on the spot key. The most in style pair wise key pre-distribution answer is Random Pair wise Key theme which addresses unessential storage drawback and provides some key resilience. It's supported Erodes and Reni's work. Every sensing element node stores a random set of Nape pair-wise keys to achieve chance  $p$  that 2 nodes are connected. Neighboring nodes will tell if they share a common pair-wise

key once they send and receive "Key Discovering" Message inside radio range. Its defect is that it sacrifices key property to decrease the storage usage. Closest (location-based) pair-wise keys pre-distribution theme is another to Random pair wise key scheme. It takes advantage of the situation data to enhance the key connectivity. Later on, Random key-chain based mostly key pre-distribution answer is another random key pre-distribution solution that originated from the answer of basic probabilistic key redistribution scheme. It depends on probabilistic key sharing among the nodes of a random graph.

There are many key reinforcement proposals to strengthen security of the established link keys, and improve resilience. Objective is to firmly generate a novel link or path key by using established keys, so the secret's not com- secure once one or a lot of sensing element node is captured. One approach is to extend quantity of key overlap needed in shared key discovery phase. Q-composite random key pre distribution theme needs letter common keys to establish a link key. Similar mechanism is projected by Pair-wise key institution protocol that uses threshold secret sharing for key reinforcement. The key reinforcement solutions in general increase process and communication quality; however give smart resilience in the sense that compromised key-chain doesn't directly have an effect on security of any links within the WSN. But, it should be doable for Associate in Nursing oppose to re- cowl initial link keys. Associate in Nursing oppose will then recover strengthened link keys from the recorded multi-path reinforcement messages once the link keys are compromised. Symmetric key schemes don't seem to be viable for mobile detector nodes and so past approaches have targeted solely on static WSNs. a couple of approaches are planned supported PKC to support dynamic WSNs.

we review previous PKC-based key management schemes for dynamic WSNs and analyze their security weaknesses or disadvantages. Chuang et al. and Agawam et al. planned a two-layered key management theme and a dynamic key update protocol in dynamic WSNs supported the Daffier Hellman (DH), severally. However, both schemes don't seem to be fitted to sensors with restricted resources and area unit unable to perform valuable computations with massive key sizes (e.g. a minimum of 1024 bit). Since computer code is computationally additional l economical and features a short key length (e.g. 160 bit), many approaches with certificate are planned supported computer code. However, since every node should exchange the certificate to ascertain the pair wise key and verify every other's certificate before use, the communication and computation overhead increase dramatically. Also, the BS suffers from the overhead of certificate management. Moreover, existing schemes don't seem to be secure. Alagheband et al. planned a key management theme by victimization ECC based signcryption, but this theme is insecure against message forgery attacks .Huang et al. planned a ECC-based key institution scheme for self-organizing WSNs. However, we tend to found the security weaknesses of their theme. In step a pair of of their theme, a detector node U sends  $z = qU \cdot H(\text{Mackey}) + dU$  (mown) to the opposite node V for authentication, wherever  $qU$  may be a static personal key of

U. But, once V receives the z, it can disclose  $qU$ , as a result of V already got Mackey and  $dU$  in step one. So, V will simply acquire  $qU$  by computing  $qU = (z - dU) \cdot H(\text{Mackey})^{-1}$ . Thus, the detector node's private secret is exposed to the opposite node throughout the key establishment between 2 nodes. Zhang et al. [10] planned a distributed settled key management theme supported ECC for dynamic WSNs. It uses the isosceles key approach for sharing the pair wise key for existing nodes and uses an asymmetric key approach to share the pair wise keys for a new node when readying. However, since the initial key KI is used to figure the individual keys and also the pair wise keys after readying for all nodes, if a soul obtains KI, the adversary has the flexibility to figure all individual keys and the pair wise keys for all nodes. Thus, such theme suffers from weak resilience to node compromises. Also, since such theme uses a straightforward ECC-based DH key agreement by victimization every node's semipermanent public key and personal key, the shared pair wise secret is static and as a result, is not secure against known-key attacks and can't give re-key operation use a ECDSA theme to verify the identity of a cluster head and a static EC-DiffieHellman key agreement theme to share the pair wise key between the cluster heads. Therefore, the theme by Duet al. isn't secure against known-key attacks, as a result of the pair wise key between the cluster heads is static. On the opposite hand, Du et al. use a standard arithmetic-based isosceles key approach to share the pair wise key between a detector node and a cluster head. Thus, a detector node cannot directly establish a pair wise key with different detector nodes and, instead, it needs the support of the cluster head. In their theme, in order to ascertain a pair wise key between two nodes within the same cluster, the cluster head arbitrarily generates a pair wise key and encrypts it victimization the shared keys with these two nodes. Then the cluster head transmits the encrypted pairwise key to every node. Thus, if the cluster head is compromised, the pair wise keys between non-compromised detector nodes in the same cluster will be compromised.

### III. PROPOSED TECHNIQUE

The most effective key for dynamic WSNs is Certificate less effective key management protocol(CL-EKM), it supports four styles of keys every of them square measure used for various functions, particularly for as well as secure pairwise node communication and group-oriented key communication among the clusters. This schema uses the most algorithms of the CL-HSC theme to derive certificate less public/private keys and pair-wise keys. It conjointly take the advantage of ECC keys outlined on associate additive cluster with a 160-bit length. the kinds of key square measure Certificate less public/private key, Individual nodes key, Pairwise key and Cluster key. Certificate less public/private key: this key generates a reciprocally documented pair-wise key. Individual node key: every node can have individual key. Pairwise key: to possess a secure communication and authentication of nodes every node shares a unique pairwise key with the neighboring nodes. Cluster key: All the nodes in a very cluster share a key and these keys square measure named as cluster key. The special organization of the

complete personal/public key pairs removes the requirement for certificates and conjointly resolves the key escrows issues by eliminating the responsibility for the users full private key, figure one explains the generation of CL-EKM and movement of nodes. Compared to alternative approach the planned schema provides additional security, decrease overhead and defend information confidentiality and integrity Security analysis of CL-EKM, security of CL-HSC uses a building block of CL-EKM, therefore CL-EKM achieves our security goals. The CL-HSC provides each confidentiality and unforgetability for signcrypted messages supported the trait of the EC-CDH. Moreover, it's insufferable to forget or expose the complete personal key of associate entity supported the issue of EC-CDH, while not the information of each KGC's master personal key associated an entity's secret price. Therefore, the confidentiality is outlined as sameness against reconciling chosen cipher-text and identity attacks (IND-CCA2) whereas unforgetability is outlined as existential unforgetability against reconciling chosen messages and identity attacks (EUF-CMA).

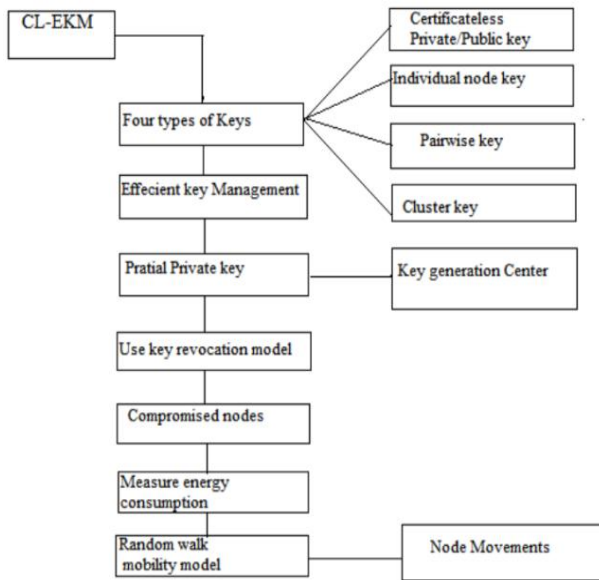


Fig 1: System flow architecture

IV. CONCLUSION

In this paper, we tend to propose the Certificate less Active Key Management Protocol (CL-AKM) to support effective key revocation for secure communication in dynamic WSNs. Key updated once a node movement of node leaves or node connections a cluster and key revocation for compromised nodes ar supported by our planned theme and ensures move and backward key confidentiality. Our planned theme of security analysis is effective during a range of attacks and robust compared to compromise node. From the simulation results, our planned theme has higher performance in terms of energy, outturn and delay. The investigational results establish the nice organization of CL-AKM to support effective key revocation is in resource controlled WSNs. Future work: associate Anonymous Location primarily based economical Routing Protocol (ALERT). ALERT dynamically partitions the networks field into regions and

arbitrarily selects nodes in regions as intermediate relay nodes, that type a non-traceable anonymous route. Therefore, ALERT suggestions namelessness protection to sources, destination, and routes. It conjointly has methods to effectively counter intersection and temporal arrangement attacks.

REFERENCES

- [1] X. Cao and G. Chen, "ROSS: Resource Oriented Security Solution for Heterogeneous Clustered Sensor Networks," *Int. J. of Intelligent Control and Systems*, 12(4):317- 324, 2007.
- [2] H. W. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," in: *Proceedings of IEEE Symp. on Security and Privacy*, 197-215, Berkeley, CA, 2003.
- [3] M. Eltoweissy, M. Heydari, L. Morales, and H. Sudborough, "Combinatorial Optimization for Key Management in Secure Multicast Environments," *Journal of Network and System Management*, 12(1):33-50, 2004.
- [4] M. Eltoweissy, M. Younis, and K. Ghumman, "Lightweight Key Management for Wireless Sensor Networks," *IEEE International Conference on Performance Computing and Communications*, 813-818, 2004.
- [5] M. R. Alagheband and M. R. Aref, "Dynamic and secure key manage-ment model for hierarchical heterogeneous sensor networks," *IET Inf. Secur.*, vol. 6, no. 4, pp. 271–280, Dec. 2012.
- [6] D. S. Sanchez and H. Baldus, "A deterministic pairwise key pre-distribution scheme for mobile sensor networks," in *Proc. 1st Int. Conf. SecureComm*, Sep. 2005, pp. 277–288.
- [7] I.-H. Chuang, W.-T. Su, C.-Y. Wu, J.-P. Hsu, and Y.- H. Kuo, "Two-layered dynamic key management in mobile and long-lived cluster-based wireless sensor networks," in *Proc. IEEE WCNC*, Mar. 2007, 4145– 4150.
- [8] B. Lai, S. Kim, and I. Verbauwhede, "Scalable Session Key Construction Protocol for Wireless Sensor Networks," *IEEE Workshop on Large Scale Real-time and Embedded Systems (LARTES)*, Austin, TX, 2002.
- [9] A. Manjeshwar and D. Grawal, "TEEN: A protocol for enhanced efficiency in wireless sensor networks," In: *Proceedings of the 15th Parallel and Distributed Processing Symp.* San Francisco, CA: IEEE Computer Society, 2009–2015, 2001.
- [10] M. Moharram, R. Mukkamala, and M. Eltoweissy, "TKGS: Threshold-based Key Generation Scheme for Wireless Ad Hoc Networks," in: *Proceedings of the IEEE International Conference on Computer Communications and Networking (ICCCN'2004)*, Chicago, IL, 31-36, October 2004.



M. Akhila Kumari Currently doing M.Tech in Computer Science and Engineering at Balaji Institute of Engineering & Science, Warangal, India. Research interests include Networks, Mobile Computing etc.,



Vishnu Prasad Goranthala Completed Master of Technology in Computer Science and Engineering from JNTU Hyderabad. Currently working as an Associate Professor at Balaji Group of Institutions, Narsampet, Warangal, and has 13+ years of experience in Academic. His research areas include Information Security, Mobile and Cloud computing, Cryptography, Network Security.