International Journal of Science Engineering and Advance Technology

A NEW EXTENSIBLE KEY EXCHANGE SCHEME FOR WIRELESS SENSOR NETWORKS

1B.kalpana(email: kalpana1207@gmail.com), 2N.Siva Rama Krishna Prasad(nsrkp.m.tech@gmail.com)
1,2Dept of **C.S.E,** S.R.K. Institute Of Technology, Enikepadu, Krishna dist, AP, India

Abstract:-A sensor network is confident of a large number of sensor nodes Sensor nodes are small, low-cost, low-power devices that have following performance communicate on short distances sense environmental data perform limited data processing The network usually also contains "sink" node which connects it to the outside world. Advances in technology introduce new application areas for sensor networks. Foreseeable wide deployment of mission critical sensor networks creates concerns on security issues. Security of large scale slowly deployed and infrastructure-less wireless networks of resource limited sensor nodes requires efficient key distribution and management mechanisms. We consider distributed and hierarchical wireless sensor networks where unjust, multicast and broadcast type of communications can take place. We evaluate deterministic, probabilistic and hybrid type of key pre-distribution and dynamic key generation algorithms for distributing combination and network-wise keys.

Keywords: Wireless sensor networks, security, key management, network scalability, secure connectivity coverage.

Introduction:-

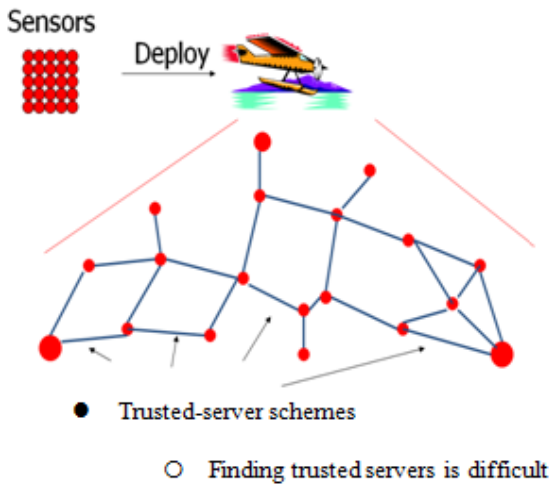
Sensors are inexpensive, low-power devices which have limited resources [Akyildiz et al. 2002]. They are small in size, and have wireless communication capacity within short distances. A sensor node typically contains a power unit, a belive unit, a processing unit, a storage unit, and a wireless transmitter / receiver. A wireless sensor network (WSN) is composed of large number of sensor nodes with limited power, computation, storage and communication capabilities. Environ-ments, where sensor nodes are deployed, can be composed (comparable as home, office, warehouse, forest, etc.) or uncontrolled (such as hostile or horm areas, toxic regions, etc.). If the environment is known and under control, deployment may be achieved manually to establish an framework. However, manual deployments become infeasible or even impossible as the number of the nodes increases. If the environment is uncontrolled or the WSN is very large, deployment has to be per-formed by randomly scattering the sensor nodes to destination area. It may be possible to provide denser sensor deployment at specific spots, but exact positions of the sensor nodes can not be controlled. Thus, network topology can not be known precisely prior to deployment. Although topology information can be obtained by using mobile sensor nodes and self-deployment protocols as proposed in [Wang et al. 2004] and [Zou and Chakrabarty 2003], this may not be possible for a large scale WSN. Security in WSN has six challenges: (i) wireless nature of communication, (ii)resource limitation on sensor nodes, (iii) very large and dense WSN, (iv) lack of fixed infrastructure, (v) unknown network topology prior to deployment, (vi) high risk of physical attacks to unattended sensors. Moreover, in some deployment scenarios sensor nodes need to operate under adversarial condition. Security solutions for such applications depend on existence of strong and efficient key distribution mechanisms. It is infeasible, or even impossible in uncontrolled environments, to visit large number of sensor nodes, and change their configuration. Moreover, use of a single shared key in whole WSN is not a good idea because an adversary can easily obtain the key. Thus, sensor nodes have to adapt their environments, and establish a secure network by: (i) using pre-distributed keys or keying materials, (ii) exchanging information with their immediate

neighbors, or (iii) exchanging in-formation with computationally robust nodes. Although there are ongoing works [Malan et al. 2004; Gaubatz et al. 2004; Huang et al. 2003] to customize public key cryptography and elliptic key cryptography for low-power devices, such approaches are still considered as costly due to high processing requirements. Key distribution and management problem in WSN is difficult one, and requires new approaches. Motivation of this paper is to evaluate the key distribution solutions. Depending on application types, it is possible to discuss: (i) network architectures such as distributed or hierarchical, (ii) communication styles such as pair-wise (unicast), group-wise (multicast) or network-wise (broadcast), (iii) security requirements such as authentication, confidentiality or integrity, and (iv) keying requirements such as pre-distributed or dynamically generated pair-wise, group-wise or network-wise keys. In this paper, we provide a comparative survey, and taxonomy of solutions. It may not be always possible to give strict quantitative comparisons; however, there are certain metrics, as described in the next section, that can be used to evaluate the solutions.

Key Management Goals:

- The protocol must establish a key between all sensor nodes that must exchange data securely
- Node addition / deletion should be supported
- It should work in undefined deployment environment
- Unauthorized nodes should not be allowed to establish communication with network nodes

Key Management Problem:



- Trusted-server schemes
  - Finding trusted servers is difficult
- Public-key schemes
  - Expensive and infeasible for sensors
- Key pre-distribution schemes

Key Pre-distribution

- Loading Keys into sensor nodes *prior to* deployment
- Two nodes find a common key between them after deployment
- Challenges
  - Memory/Energy efficiency
  - Security: nodes can be compromised
  - Scalability: new nodes might be added later

Straight Forward Approach:

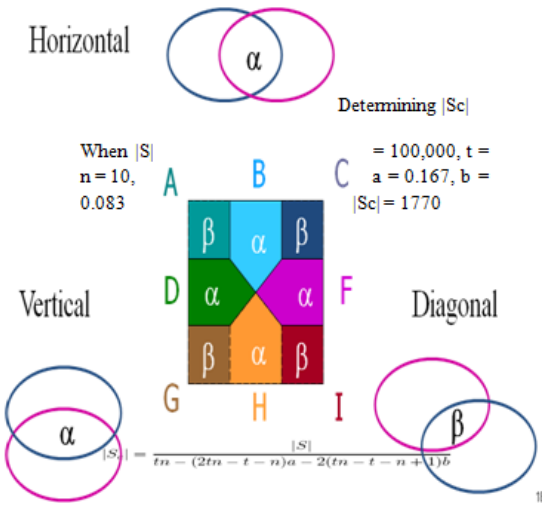
- Single mission key is obviously unacceptable

- Pairwise private key sharing between every two nodes is impractical because of the following reasons:
    - it requires pre-distribution and storage of n-1 keys in each node which is n(n-1)/2 per WSN
    - most of the keys would be unusable since direct communication is possible only in the nodes neighborhood
    - addition / deletion of the node and re-keying are complex

Basic Probabilistic Approach:

- Proposed by Eschenauer and Gligor
- Relies on probabilistic key sharing among nodes of WSN
- Uses simple shared-key discovery protocol for key distribution, revocation and node re-keying
- Three phases are involved: key pre-distribution, shared-key discovery, path-key establishment

Key Pre-distribution



Shared-key Discovery:-

- Takes place during initialization phase after WSN deployment. Each node discovers its neighbor in communication range with which it shares at least one key
- Nodes can exchange IDs of keys that they poses and in this way discover a common key
- A more secure approach would involve broadcasting a challenge for each key in the key ring such that each challenge is encrypted with some particular key. The decryption of a challenge is possible only if a shared key exists

Path-key Establishment:-

- During the path-key establishment phase path-keys are assigned to selected pairs of sensor nodes that are within communication range of each other, but do not share a key
- Find secure path by using flooding method

n = 4

t = 4				
	1	1 – a	1 – a	1 – a
	1 – (a+b)	1 – 2(a+b)	1 – 2(a+b)	1 – (2a+b)
	1 – (a+b)	1 – 2(a+b)	1 – 2(a+b)	1 – (2a+b)
	1 – (a+b)	1 – 2(a+b)	1 – 2(a+b)	1 – (2a+b)

Fig:Key Assignment for all the key pools

    - Limit the lifetime of the flooding message to three hops to reduce flooding overhead
- Share random key K by using secure path

Local Connectivity:-

- With 100 keys, location management improves local connectivity from 0.095 to 0.687

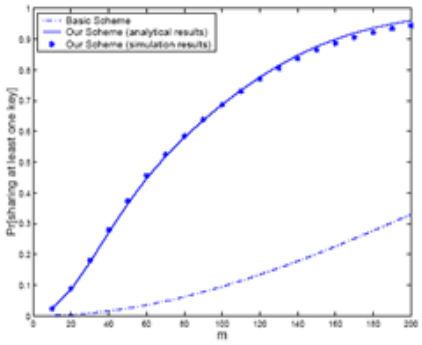


fig:Local connectivity: Probability of sharing atleast one key between two neighbouring nodes.

Conclusion:-

Robust security mechanisms are vital to the wide acceptance and use of senor networks for many applications Security in WSN is quite different from traditio(wired) network security Various peculiarities of WSN make the development of good key scheme a challenging task We have discussed several approaches to key management in WSN.

References:

[1] Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah, and Vahid Tarokh "A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks," in IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 2, FEBRUARY 2013.

[2] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: asurvey," *IEEE Commun. Surv. Tuts.*, vol. 10, no. 1–4, pp. 6–28, 2008.

[3] L. Eschenauer and V. D. Gligor, "A key-management scheme fordistributed sensor networks," in *Proc. 2002 ACM CCS*, pp. 41–47.

[4] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemesfor sensor networks," in *IEEE SP*, pp. 197–213, 2003.

[5] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key managementscheme for wireless sensor networks using deployment knowledge," in*Proc. 2004 IEEE INFOCOM*, pp. 586–597.

[6] C. Castelluccia and A. Spognardi, "A robust key pre-distribution protocolfor multi-phase wireless sensor networks," in *Proc. 2007 IEEESecurecom*, pp. 351–360.

[7] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensorbetworks," in *Proc. 2003 ACM CCS*, pp. 52–61.

[8] Z. Yu and Y. Guan, "A robust group-based key management scheme for wireless sensor networks," in *Proc. 2005 IEEE WCNC*, pp. 1915–1920.

[9] S. Ruj, A. Nayak, and I. Stojmenovic, "Fully secure pairwise andtriple key distribution in wireless sensor networks using combinatorial designs," in *Proc. 2011 IEEE INFOCOM*, pp. 326–330.

[10] S. Zhu, S. Setia, and S. Jajodia, "Leap: efficient security mechanisms for large-scale distributed sensor networks," in *Proc. 2003 ACM CCS*,pp. 62–72.

[11] S. A. C¸ amtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," *IEEE/ACM Trans. Netw.*,vol. 15, pp. 346–358, 2007.

[12] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar, "Spins: security protocols for sensor networks," in *Proc. 2001 ACM MOBICOM*,pp. 189–199.

[13] B. Maala, Y. Challal, and A. Bouabdallah, "Hero: hierarchcal keymanagement protocol for heterogeneous WSN," in *Proc. 2008 IFIPWSAN*, pp. 125–136.

Miss. Bandikalla Kalpana is a student of S.R.K Institute Of Technology, Enikepadu .Presently she is pursuing her M.Tech [Computer Science Engineering] from this college and she received his B.Tech from Vasavi College of Engineering, Thadepalligudem, affiliated to JNT University, Kakinada in the year 2011. Her area of interest includes Information Security, Computer Networks and Data Warehouse & Data Mining, all current trends and techniques in Computer Science

Mr.N.Siva Rama Krishna Prasad, well known Author and excellent teacher Recieved M.Tech from Vasavi Engineering College is working as Associate Professor, Department of CSE, S.R.K Institute Of Technology. He has 2 years of teaching experience in engineering college. To his credit couple of publications both national and international conferences /journals . His area of Interest includes Data Warehouse and Data Mining, information security, flavours computer Applications.