RESEARCHERID
THOMSON REUTERS

[Saxena* *et al.*, 6(7): July, 2017]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SURVEY OF SECURED APPROACH TO ROUTING IN WIRELESS SENSOR NETWORKS USING THRESHOLD CRYPTOGRAPHY

Shraddha Saxena[*1] & Rohit Kumar Rathor[2]
[*1]M.Tech Student, Department of ECE, LNCTE, Bhopal, India
[2]Asst. Professor, Department of ECE, LNCTE, Bhopal, India

DOI: 10.5281/zenodo.829791

ABSTRACT

In this paper, characteristics of Wireless Sensor Networks (WSN), along with problems and security issues usually faced in routing Wireless sensor networks due to highly dynamic nature and lack of centralized management and infrastructure has been tried to explore. The main objective of this paper is to put an effort to improve security in routing protocols, especially Clustered routing Protocol using concepts of Threshold Cryptography of distributed key management and certification. Since providing security support for ad hoc wireless networks is challenging for a number of reasons such as susceptibility to security attacks ranging from passive eavesdropping to active interfering and denial-of-service (DoS) attacking. Wireless sensor networks are prone to occasional break-ins in a large-scale mobile network are inevitable over a large time interval. Such networks provide no infrastructure support. Adequate security support for authentication, confidentiality, integrity, non-repudiation, access control and availability is critical to deploying this wireless networking technology in commercial environments. Today, networks security, whatever they are wireless or not, is an important component in the network management. The works done and studied so far are limited either up to one hop networks or for application layer services only. This work thus has been proposed to implement threshold cryptography over Clustered Based Routing Protocol and to study its behavior of packet flow on the basis of Throughput, packet delivery ratio, Normalized Routing overhead and End to end delay in different scenario and compared with the scenario without implementing the security.

KEYWORDS: Wireless Sensor Networks, Mobile Ad Hoc Networks, Key Management, Threshold Cryptography, Clustered Routing.

I. INTRODUCTION

"A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location."

Advancements in Micro-Electro-Mechanical Systems(MEMS), low-power electronic devices integrated with wireless communication capabilities and sensors are stimulating the growth of wireless sensor networks (WSN) across diverse applications [2]. A wireless sensor network is a collection of large number of inexpensive, tiny, autonomous wireless devices called as sensor nodes. These nodes, commonly known as motes, which are substantially smaller in size than hand-held devices such as mobile phones, or personal digital assistants (PDAs). The WSNs are randomly deployed in large physical space to monitor physical and environmental conditions, often in real time, such as temperature, pressure, light, humidity, chemical level and fire detection [3].

In spite of similarities among WSNs and MANETs, there are also some fundamental differences between these two networks. The differences listed here are:

- The number of sensor nodes in a WSNs is in the order of several hundreds to thousands compared to small number in MANETs.
- Nodes are densely deployed in WSNs.
- Nodes in WSNs are prone to failure due to physical and environmental conditions.
- The topology of a WSN changes very frequently due to nodes failure.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

- In Most of the applications, sensor nodes use broadcast communication paradigms whereas MANETs are based on point-to-point communications.
- In WSNs, nodes are resource constrained i.e limited power, computational capabilities, and memory.
- Nodes in WSNs may not have global unique identification because of the large number of nodes.
- In most of the WSNs applications, mobility of sensor nodes are relatively low or nil as compared to MANETs.
- Data rate is very low in WSNs.
-

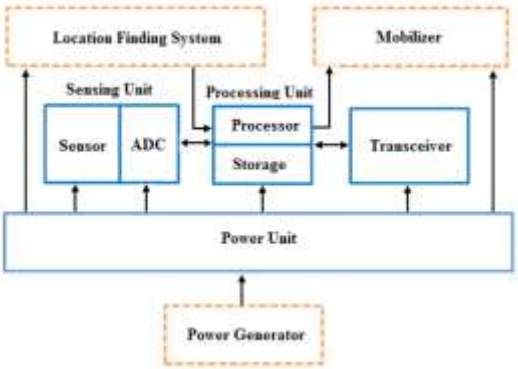

Fig 1 Components of typical sensor nodes

II. LITERATURE REVIEW

Most of the traditional techniques, however, are unsuitable in low power devices such as WSNs. This is due largely to the fact that typical key exchange techniques use asymmetric cryptography, also called public key cryptography. In this case, it is necessary to maintain two mathematically related keys, one of which is made public while the other is kept private. This allows data to be encrypted with the public key and decrypted only with the private key. The problem with asymmetric cryptography, in a wireless sensor network, is that it is typically too computationally intensive for the individual nodes in a sensor network.

The LEAP protocol described by Zhu et. al. [34]. They have followed an different approach that utilizes multiple keying mechanisms. Their observation is that no single security requirement accurately suites all types of communication in a wireless sensor network. Therefore, four different keys are used depending on whom the sensor node is communicating with. Sensors are preloaded with an initial key from which further keys can be established. As a security precaution, the initial key can be deleted after its use in order to ensure that a compromised sensor cannot add additional compromised nodes to the network.

In [18], described a mechanism for establishing a key between two sensor nodes that is based on the common trust of a third node somewhere within the sensor network. The nodes and their shared keys are spread over the network such that for any two nodes A and B, there is a node C that shares a key with both A and B.

Liu. D and Ning. P, in [31] proposed an enhancement to the µTesla system that uses broadcasting of the key chain commitments rather than µTesla's unicasting technique. They present a series of schemes starting with a simple pre-determination of key chains and finally settling on a multi-level key chain technique. The multi-level key chain scheme uses pre-determination and broadcasting to achieve a scalable key distribution technique that is designed to be resistant to some types of wireless sensor network attacks.

III. THRESHOLD CRYPTOGRAPHY

In classic cryptography, a private key is secretly held by a user and must never be revealed, if not, security system wouldn't be reliable. Instead, in threshold cryptography, the secret is shared between several network nodes, in such a way no single node can deduce the secret without the knowing of the whole shares. The principal benefit in using threshold cryptography is to ensure security services by employing encryption without keeping the secret at only one holder, which could easily compromise.

The idea of Shamir's (k, n) threshold system is to share a secret key between n parties [3].

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Each group of any k participants (share holders), can cooperate to reconstruct the shares and recover the secret. On the other hand, no group of k-1 participants can get any information about the secret.

The Shamir's (k, n) threshold theory is the following:

If we consider s the secret, such as s ϵ ?p, and p prime, we have to select a random polynomial f , such as:

$f(x) = f_0 + f_1x^2 + \ldots + f_{k-1}x^{k-1}$, under the condition that f (0) = s.
Where $f_1, \ldots f_{k-1} \leftarrow$randomly
$f_0 \leftarrow s$
For i Є [1, n], the shares $s_i$are distributed as: $s_i = (i, f(i))$
The Shamir's (k, n) threshold theorem stipulates that the secret s can be reconstructed from every subset of k shares. This is proven by the Lagrange formula. In fact, given k points (x_i, y_i), i = 1, . . . , k, .

And thus

The Shamir's (*k*, *n*) threshold scheme announces a second theorem stipulating that any subset of up to *k*-1 shares does not leak any information on the secret. Indeed, when considering *k*-1 shares (x_i, y_i), every candidate secret *s*′Є?*p* corresponds to an unique polynomial of degree *k*-1 for which *f* (0) = *s*′. From the construction of polynomials, for all *s* Є ?*p*, probabilities Pr[*s* = *s*′] are equal. The theorem is then proven.

IV. CLUSTERED ROUTING

As a result of advances in wireless technology and widespread application of wireless mobile ad hoc networks, the scale of network topology is increasing at unbelievable pace. Wireless mesh networks own large dense nodes and desires the characteristics such as self configuration, robustness, easy maintenance, low cost and most importantly Scalability [9]. Here comes the role of Hierarchical routing or what we commonly known as Clustered routing structures. Clustered Routing Structures have many prominent advantages, such as [9]:

1. During the routing, path-building phase, clustering mechanism dramatically reduces flooding overhead by decreasing the retransmission of broadcast packets.
2. During the data transmitting phase, messages that flow through the network van be further reduced by aggregating data within clusters.
3. During Routing maintenance phase, clustering mechanism made it easy to manage and handle the network changes caused by node mobility and local changes need not be seen by entire network.

Clustering approach is used to minimize on-demand route discovery traffic. The idea behind CBRP is to divide nodes of an ad hoc network into a number of overlapping or disjoint clusters. One node is elected as cluster head for each cluster. The cluster head maintains membership information for its cluster. Inter cluster routes are discovered dynamically using the membership information.

The difference is that the cluster structure generally means that the number of nodes disturbed is much less. Flat routing protocols, i.e. only one level of hierarchy, might suffer from excessive overhead when scaled up. [13]

V. PROPOSED WORK

The work we presented here for key management in ad hoc networks and implemented it at routing layer in ad hoc networks, assume the existence of a clustering protocol which can split the network into groups that are stable enough. It uses a (K,N) threshold scheme to distribute an RSA certificate signing key to the set of cluster heads. It also uses proactive and verifiable secret sharing (which is out of the scope of this work) to protect the secret respectively from denial of service attacks and node compromise.
This architecture consists of 3 types of nodes

- Set of Cluster heads- which will provide distributed CA services
- Simple nodes.
- Administrator.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

1. **Cluster Generation Step**:

We are not going to propose a new clustering protocol but to select an existing one (WCA, H-ID, Min-ID..[9].) which would be suitable for our case study concerning key management. Clustering parameters that we must take into consideration are:

- ***Clusters stability:*** We prefer having clusters where the corresponding cluster heads have a minimum mobility degree.
- ***Cluster heads energy*****:** we had better to elect cluster heads having the highest power because they will be responsible for some tasks.

2. **Initialization**: At Initialization, we assume some mechanism proposed earlier in [2], [12], [14] [24] to distribute shares among cluster heads in our network at initial step and after that such responsibility is handed over to set of cluster heads sharing secret. Thus every CH, C_i will then possess a secret key S_i of the CA secret key which helps in securing network and handling of secret in an efficient manner. Cluster head will be then considered as a distributed CA for further scaling of network.

Following section consists of firstly an algorithm for secret sharing, i.e. it shows how a secret will be distributed over a number of shares when administrator is not present in system.

3. **Algorithm Key Sharing**

- New CH contacts to administrator.
- If latter is present, CH sends a request for initialization including its id and public key, else
- goto (5).

4. **Administrator computes a partial key to CH in following way:**

- Select a large prime number p.
- Consider a polynomial function f(x) of degree k-1 such that
  $f(x)= [S+a_1x+a_2x^2+ \ldots + a_{k-1}x^{k-1}] \bmod p$,
  where k is number of nodes among which secret has been shared.
- Now, compute the partial key $S_i = f(id)$, where id is identity provided by the CH.

5. CH sends request any cluster head (shareholders) CHL, which on certifying issue him, his partial share in the following way:

- $S_{CH,I} = S_L$ X $Fid_L(id)$, where
- By combining, k such shares i.e. $S_{CH,I}$, we get, S_i as follows:
  $= f(id)$

6. Endif

7. End.

VI. CONCLUSION

The present work is carried in the general context of security study in wireless sensor networks and focused on key management problem in such networks and tried to implement it and evaluate it through Threshold Cryptography concept proposed by Shamir by employing it on Clustered Routing Protocol. The work consists in analyzing effects of employing secret sharing mechanism over clustered routing in wireless sensor networks to palliate their limitations which ensures better and secure environment.

VII. REFERENCES

[1] K. Akkaya, M. Younis, "A Survey of Routing Protocols in WSNs", Elsevier, Ad Hoc Network Journal, Vol. 3, No.3, pp. 325-349, 2005.
[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, Vol. 40, No.8, pp. 102-114, August 2002.
[3] Adi Shamir, Massachusetts Instt of Technology, "How to Share a secret".
[4] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "WSNs: A Survey", Computer Networks, Vol. 38, No.4, pp. 393-422, 2002.
[5] Charles E. Perkins, "Ad Hoc Networking" Pearson Education, 2001.
[6] Brain P. Crow, IndraWidjaja, JeonGeun Kim and Prescott T. Sakai, "IEEE802.11 Wireless Local Area Networks", IEEE Communication Magazine, Vol.35, Sep 1997

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

[7] J. Macker and S. C. (chairmen). MANET (Mobile Ad Hoc Networking) working group of the IETF
[8] Renu Bala1 and Dr. Yashpal Singh "Secure Routing in Wireless Sensor Network. ",International Journal of Computer Science and Mobile Computing ,IJCSMC, Vol. 4, Issue. 5, May 2015, pg.966 – 973

CITE AN ARTICLE

Saxena, Shraddha , and Rohit Kumar Rathor. "A SURVEY OF SECURED APPROACH TO ROUTING IN WIRELESS SENSOR NETWORKS USING THRESHOLD CRYPTOGRAPHY." ***INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*** **6.7 (2017): 606-10. Web. 15 July 2017.**