ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Certificate Revocation For Load Balanced Clusters in Wireless Sensor Networks

[I]S. Santhiya, [II]B.Preetha, [III]B.Anitha
[I]PG Student, CSE, Vivekanandha College of Engineering for Women, Namakkal, India
[II,III]Assistant Professor, CSE, Vivekanandha College of Engineering for Women, Namakkal, India

Abstract
Wireless sensor network (WSN) contains large number of tiny sensors that can be used as an effective tool for gathering data in diverse kinds of environments. To support data aggregation and high scalability, sensor nodes are often grouped into non overlapping subsets called clusters. Clustering of sensor nodes into groups saves energy and also reduces network contention when nodes communicate over shorter distances with their respective cluster-head. The clustering of nodes can be compromised or misbehaved by adversaries which leads to security problem. Certificate revocation mechanisms play an important role in securing a network. When the certificate of a malicious node is revoked, it is denied from all activities and isolated from the network. The main challenge for certificate revocation is to revoke the certificates of malicious nodes promptly and accurately. In this paper, proposed scheme is based upon a clustering-based certificate revocation scheme, which outperforms other techniques in terms of being able to quickly revoke attackers certificates and recover falsely accused certificates.

Keywords
Residual energy, Wireless Sensor Networks, Certificate authority, Certificate revocation.

I. Introduction

Wireless sensor networking is an emerging technology that enables the deployment of wireless sensor networks (WSNs) for a wide range of applications such as environment monitoring, tracking of objects and data collection. Sensor nodes in WSNs are usually battery-powered and expected to operate for a long period. Moreover, in many applications, it is not possible to recharge batteries once the sensor nodes have been deployed. Therefore, energy is a vital resource in low power wireless sensor networks, and energy consumption should be well managed in wireless sensor networks, and consumption of energy should be managed to prolong the post-deployment network lifetime. Clustering protocols is used for conserving the energy from the deployment of sensor nodes. Clustering is an essential part of the organizational structure, Consequently, the cluster nodes is vulnerable to many kinds of malicious attacks, and it is thus difficult to ensure secure communications Malicious nodes directly threaten the robustness of the network as well as the availability of nodes. Protecting legitimate nodes from the malicious attacks must be considered in WSNs. This is achievable through the use of a key management scheme which conveying trust in a public key infrastructure. These certificates are signed by the Certificate Authority (CA) of the network, which is a trusted third party that is responsible for issuing and revoking certificates. The mechanism performed by the CA plays an important role in enhancing network security. It digitally signs a valid certificate for each node to ensure that nodes can communicate with each other in the network. In such networks, a certificate revocation scheme which invalidates attackers certificates is essential in keeping the network secured. An attacker's certificate can be successfully revoked by the CA if there are enough accusations showing that it is an attacker. However, it is difficult for the CA to determine if an accusation is trustable because malicious nodes can potentially make false accusations. A malicious node will try to remove legitimate nodes from the network by falsely accusing them as attackers. Therefore, the issue of false accusation must be taken into account in designing certificate revocation mechanisms.

II.Related Work

In DSBCA (Balanced Clustering Algorithm with Distributed Self-Organization for Wireless Sensor Networks) clusters are generated in both uniform and non-uniform distribution with more balanced energy and avoid creating excessive clusters with many nodes, thus it overcomes other existing clustering algorithms. The basic idea of DSBCA is based on the connectivity density and the distance from the base station to calculate k (clustering radius). In this the two neighboring nodes receive their certificates from each other and also exchange certificate information about other nodes that they know. Nodes sharing the same certificate information are regarded as belonging to the same network. In these networks, the certificate of a suspected node can be revoked when the number of accusations against the node exceeds a certain threshold. It does not require any special equipment such as Certificate Authorities (CA), the operational cost is still high. URSA proposed by Luo et al. [5] uses certified tickets which are locally managed in the network to evict nodes. URSA does not use a third-party trust system such as a CA. The tickets of the newly joining nodes are issued by their neighbors. Since there is no centralized authority, the ticket of a malicious node is revoked by the vote of its neighbors. In URSA, each node performs one-hop monitoring and exchanges monitoring information with its neighbors which allow for malicious nodes to be identified. When the number of votes exceeds a certain threshold, the ticket of the accused node will be successfully revoked. Since nodes cannot communicate with other nodes without valid tickets, revoking a node's ticket implies the isolation of that node. In contrast to URSA, DICTATE employs a number of CAs to efficiently perform the publication and revocation of certificates. CAs monitor node behavior in order to detect attacks and share the certificate information with each other. If a CA identifies a malicious node, the certificate of the node is revoked by the CA and its information is shared among other CAs, thus resulting in the complete exclusion of the node from the network. However, the deployment of a sufficient number of CAs is not an easy task in WSNs.

III. Clustering Of Nodes

By classifying nodes into clusters, the proposed scheme allows each Cluster Head (CH) to detect false accusation by a Cluster Member (CM) within the cluster. Node clustering provides a means to mitigate false accusations. Each cluster consists of one CH and CMs lying within the CH's transmission range, some nodes within the transmission area of the CH might not be the member of the cluster and can be the CM of another cluster in the load balanced

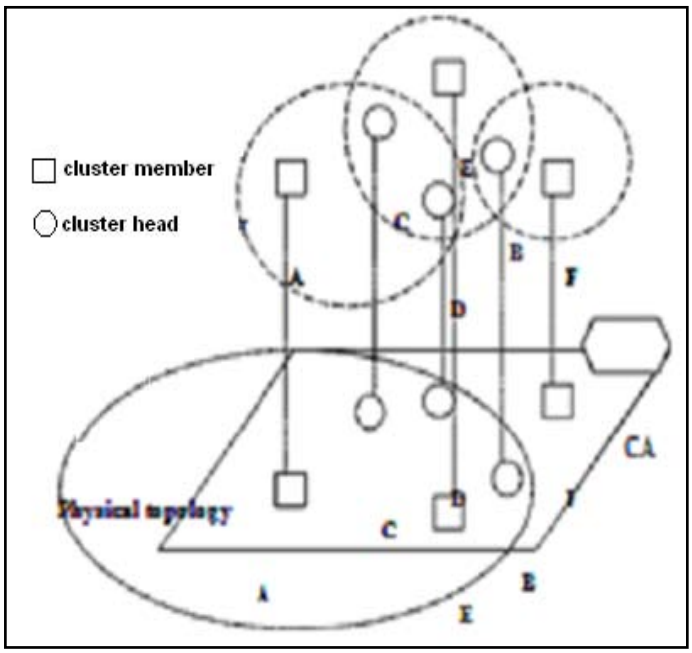

Fig.1: Node clustering

For example, in Fig. 1, node B does not belong to the cluster headed by node A while it is located within the transmission area of node A. Only normal nodes having high reliability are allowed to become a CH. Nodes except CHs join the two different clusters of which CHs exist in the transmission range of them. By constructing such clusters, each CH can be aware of false accusations against any CMs since each CH knows which CM executes attacks or not, because all of the attacks by a CM can be detected by any node, of course including the CH, within the transmission range of the CM. The reason why each node except CH belongs to two different clusters is to decrease the risk of having no CH due to dynamic node movement. To maintain clusters, CH and CMs frequently confirm their existence by exchanging messages, i.e., the CH periodically broadcasts CH Hello packets to the CMs within its transmission range, and each CM replies to the CH with the CM Hello packet.

IV .Malicious observation on adversary attack

The adversary decision on the kind of attack to launch is driven by the tradeoff between the chances of success and the freedom of choice on its fake position. The basic attack allows the adversary to choose any false position, but it requires a high percentage of colluders in the neighborhood in order to be successful. The hyperbola-based attack implies less freedom of choice but has higher chances of success. The collinear attack pins the adversary into a precise angle with the verifier, and strictly bounds its distance from the verifier itself. However, if the network topology features a sufficient number of collinear nodes, this attack has the highest success probability.

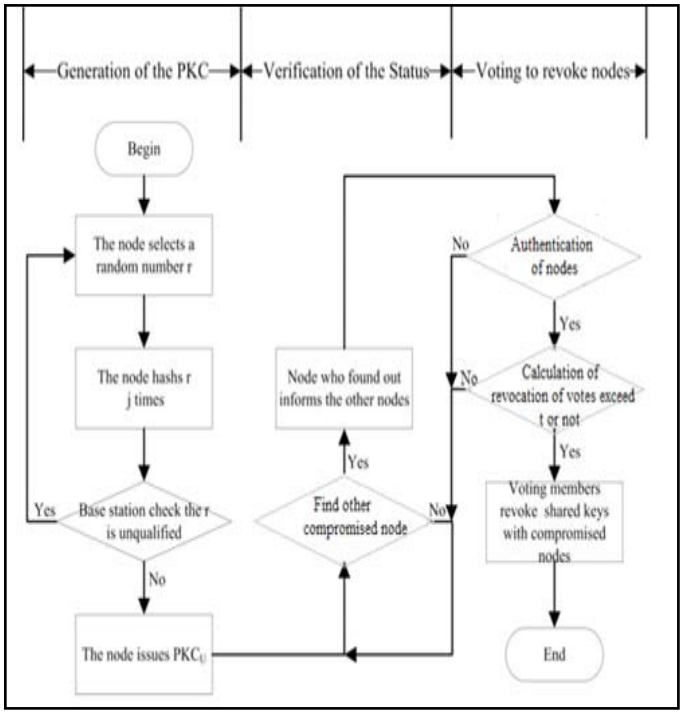

Fig. 2: Malicious observation of nodes

The colluding attackers agree not only on the position of the verifier (either guessed or multilaterated), but also pick a non collinear common neighbor, X, that they share with S: each colluder then computes the hyperbola with foci S, X, and passing through its own real position, and announces a fake location on such a curve. This allows the adversaries to announce correct links 1) with the verifier, 2) among themselves, and 3) with the selected neighbor X, which becomes an involuntary ally in the attack.

V. Clustering- based certificate revocation scheme

In this, clustering-based certificate revocation scheme which was originally proposed in [4]. Although a centralized CA manages certificates for all the nodes in the network, cluster construction is decentralized and performed autonomously. Nodes cooperate to form clusters and each cluster consists of a Cluster Head (CH) along with several Cluster Members (CMs) that are located within the communication range of their CH. Each CM belongs to two different clusters in order to provide robustness against changes in topology due to mobility. It should be noted that because the clusters overlap, a node within the communication range of a CH is not necessary part of its cluster. The aim of using clusters is to enable CHs to detect false accusations. Requests for the CA to recover the certificates of falsely accused nodes can only be made from CHs. A CH will send a Certificate Recovery Packet (CRP) to the CA to recover

an accused node, only in the case where it is a CM in its cluster. This is based on the fact that most types of attacks, such as flooding attack , black hole attack , wormhole attack and can be detected by any node within the communication range of the attacker. In other words, a CH will be able to detect any attack executed by one of its CMs, implying that a CH can identify whether a CM is malicious or not. In order for clustering-based certificate revocation to work, CHs must be legitimate. Nodes can be classified into three different categories, normal nodes which are highly trusted, warned nodes with questionable trust, and attacker nodes which cannot be trusted. Only normal nodes are allowed to become CHs

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

and accuse attackers by sending. Detection Packets (ADPs) to the CA. Nodes in the Warning List (WL) cannot become CHs or accuse attackers, but they can still join the network as CMs and communicate without any restrictions. Nodes that is classified as attackers are considered malicious and completely cut off from the network. The reliability of each nod is determined by the CA as follows. The CA maintains both Black List (BL) and a Warning List. When the CA receives an ADP from an accuser, the accused node is regarded as an attacker and is immediately registered in the BL. The BL includes nodes which are classified as attackers and have had their certificates revoked. The accuser of the attacker is then listed in the WL because the accuser might actually be making a false accusation. However, falsely accused nodes will be restored quickly by their CHs. We consider false accusation and false recovery as an act of misbehavior, and define nodes that do such act as misbehaving nodes.

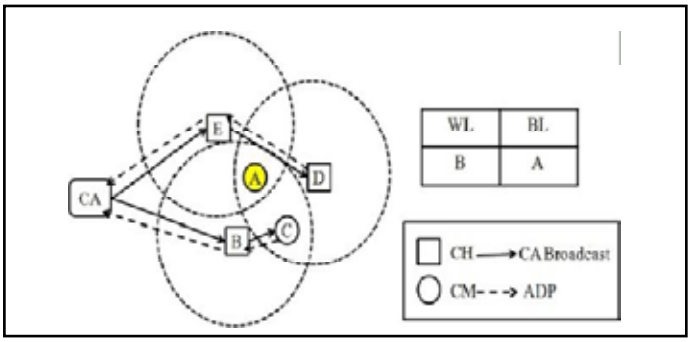

Fig.3 : The procedure of certificate revocation

Node A is a malicious node and launches attacks on its neighbors, i.e. nodes B, C, D and E. Its neighbors detect the attacks and send ADPs to the CA to accuse node A. Upon receiving the first ADP from node B, the CA puts it into the WL as an accuser and node A into the BL as an attacker. It then broadcasts the information contained in the WL and BL to the entire network.

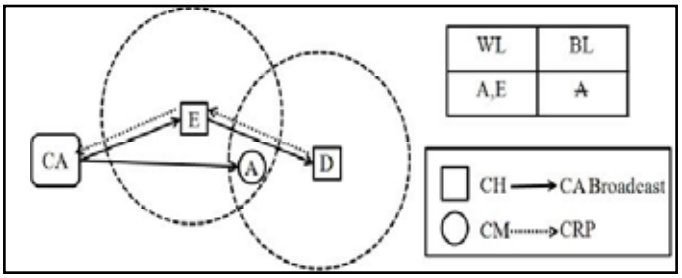

Fig. 4 : The procedure of certificate recovery

Fig.4 show the procedure of certificate recovery. When node E and D, which are the CHs of node A, are informed that node A is listed in the BL, if they have never detected any attacks coming from A, the accusation as a false one. They will then send a CRP to the CA to recover node A's certificate. Upon receiving the first arrival CRP from node E, the CA removes the falsely accused node A from the BL, and enlists it into the WL along with node E. After the broadcast of the updated WL and BL, the certificate of node A will be recovered successfully.

VI. Advantages

The proposed certificate revocation scheme for wireless sensor networks, provide some measure of protection against malicious accusation succeeding in causing the revocation of certificates of trustworthy, well-behaving nodes.

VII. Conclusion And Future Work

In this paper, we have enhanced our previously proposed clustering-based certificate revocation scheme which allows for fast certificate revocation. In order to address the issue of the number of normal nodes being gradually reduced, we have developed a threshold based mechanism to restore the accusation function of nodes in the WL. The effectiveness of our proposed certificate revocation scheme in wireless sensor networks has been demonstrated through extensive simulation results. Our future work includes doing further explorations to evaluate our protocol through security analyses and simulations to access its robustness and its cost in terms of overhead and throughput.

References

[1]. *Ying Liao, Huan Qi, and Weiqun Li(2013) Load-Balanced clustering Algorithm With Distributed Self-Organization for Wireless Sensor Networks*

[2]. *T.Panke,"Review of Certificate Revocation in Mobile Ad Hoc Networks,"International Journal of Advances in Management, Technology & Engineering Sciences,ISSN:2249-7455,vol.II,Issue 6,March 2013.*

[3]. *Y.Joshi,T.Panke,"Study of Certificate Revocation in Mobile Ad Hoc Networks,"National Conference Entitled Fostering Management and I.T.for Gen-Next,ISBN:978-81-920972-1-3.*

[4]. *H. Luo, J. Kong, P. Zerfos, S. Lu and L. Zhang, "URSA: ubiquitous and robust access control for mobile ad hoc networks," IEEE/ACM Trans. Networking, vol. 12, no. 6, pp.1049-1063, Oct. 2004.*

[5]. *W. Heinzelman, A. Chandrakasan and H. Balakrishnan, Energyefficient communication protocols for wireless microsensor networks,in: Proceedings of the 33rd Hawaiian International Conferenceon Systems Science (January 2000).*

[6]. *W. Heinzelman, A. Chandrakasan and H. Balakrishnan, An application-specific protocol architecture for wireless microsensor networks, IEEE Transactions on Wireless Communications 1(4)(2005) 660–670.*

[7]. *W. R. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "Energyefficient communication protocol for wireless micro sensor networks,"in Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci., Jan. 2000, pp. 1–10.*

[8]. *J. S. Lee and W. L. Cheng, "Fuzzy-logic-based clustering approach for wireless sensor networks using energy predication," IEEE Sensors J.,vol. 11, no. 9, pp. 2891–2897, Sep. 2012.*

[9]. *B. A. Attea and E. A. Khalil, "A new evolutionary based routing protocol for clustered heterogeneous wireless sensor networks," Appl.Soft Comput., vol. 12, no. 7, pp. 1950–1957, 2011.*

[10]. *O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," IEEE Trans. MobileComput., vol. 3, no. 4, pp. 366–379, Dec. 2004.*

[11]. *C. H. Lin and M. J. Tsai, "A comment on HEED: A hybrid, energyefficient, distributed clustering approach for ad hoc sensor networks,"IEEE Trans. Mobile Comput., vol. 5, no. 10, pp. 1471–1472, Oct. 2006.*

[12]. *Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad hoc routing," in Proc. 7th Annu. Int. Conf. Mobile Comput. Netw., Jul. 2001, pp. 70–84.*

[13]. M. Chatterjee, S. K. Das, and D. Turgut, "WCA: A weighted clustering algorithms for mobile ad hoc networks," Cluster Comput., vol. 5, no. 2,pp. 193–204, 2002.

[14]. Y. Fernandess and D. Malkhi, "K-clustering in wireless ad-hoc networks,"in Proc. 2nd ACM Workshop Principles Mobile Comput. Conf.,Oct. 2002, pp. 31–37.

[15]. H. C. Lin and Y. H. Chu, "A clustering technique for large multihop mobile wireless networks," in Proc. 51st Int. Conf. Veh. Technol., May2000, pp. 1545–1549.

[16]. M. Lehsaini, H. Guyennet, and M. Feham, "A novel cluster-based selforganization algorithm for wireless sensor networks," in Proc. Int. Symp Collabor. Technol. Syst. Conf., May 2008, pp. 19–26.

[17]. M. Youssef, A. Youssef, and M. Younis, "Overlapping multihop clustering for wireless sensor networks," IEEE Trans. Parallel Distrib. Syst.,vol. 20, no. 12, pp. 1844–1856, Dec. 2009.

[18]. J. Anno, L. Barolli, A. Durresi, F. Xhafa, and A. Koyama, "Performance evaluation of two fuzzy-based cluster head selection systems for wireless sensor networks," Mobile Inf. Syst., vol. 4, no. 4, pp. 297–312, 2008.

[19]. H. Bagci and A. Yazici, "An energy aware fuzzy unequal clusteringalgorithm for wireless sensor networks," in Proc. IEEE Int. Conf. Fuzzy Syst., Jul. 2010, pp. 1–8.

[20]. W. R. Heinzelman, "An application-specific protocol architecture for wireless microsensor networks," IEEE Trans. Wireless Commun., vol. 1,no. 4, pp. 660–670, Oct. 2002.

[21]. G. Makihara, M. Yokomichi, and M. Kono, "Design of nonlinearcontrollers for active vehicle suspension with state constraints," Artif.Life Robot., vol. 13, no. 1, pp. 41–44, 2008.