ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2 Issue Special 1 Jan-March 2014
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Protection Against Denial of Service (DoS) Attacks in Wireless Sensor Networks

[1]Dines Kumar.V.S, [2]Navaneethan.C
[1]PG Scholar, Dept. of CSE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India
[2]Assistant Professor, SITE Shool VIT University, Vellore, Tamilnadu, India

Abstract
Security could be a vital issue in Wireless device Networks (WSN) attributable to deployed in harsh and inaccessible environments for observation their several surroundings, delivering knowledge to a centralized entity, knowledge analysis, and for generating reports. WSNs ar exposed to 'Denial of Service attacks' that degrades the general Quality of Service (QoS) by endeavor the energy consumption. during this paper our planned work is associate energy-preserving answer to notice malicious and compromised nodes and a theme for preventing Denial of Service attacks in Wireless device Networks. DPDSA relies on cryptography associated hierarchic agglomeration technique that elects the Cluster Heads (CH) that analyses the traffic within a cluster and whenever an abnormal behavior is detected it sends warnings to the key distributing server. The planned methodology is dynamic because the CHs are sporadically non appointive supported the chance of changing into a cluster head and intra cluster communication price that could be a perform of node degree or cluster density among normal nodes on every atomic cluster which ends up in an exceedingly higher energy balance whereas maintaining sensible detection coverage and delay between packets transmission. The simulation results shows that the protocol for preventing DoS attacks not solely defends the wireless device network against them however additionally maintains integrity, legitimacy and confidentiality of knowledge transmitted between device nodes

Keywords
Denial of Service (DoS) attacks, Wireless Sensor Networks (WSN), cryptography, clustering-HEED

I. Introduction

Wireless Sensor Networks (WSN) consists of a large number of small and individual sensors that are capable of monitoring and sensing the environment. Due to their adaptability to various environments and low cost, wireless sensor networks have extended to many real world applications such as military surveillance, environment monitoring, aerospace, personal health care, etc. The sensor nodes send the sensed data to a base station or sink and this base station to a remote server. Sometimes the sensed data which is sensitive is send to destination node through an insecure medium. Thus, WSN can be easily attacked by Denial of Service (DoS) attacks which disrupt the wireless transmission and cause information loss. Hence providing the secured links is important in designing WSN. In DoS attacks, the adversary interfere normal operation of network by overloading the target with continuous requests such that it does not respond to legitimate traffic. The attacker's main objective is to make the target systems inaccessible by legitimate users to which they are entitled. In general a DoS attack is an explicit attempt by an adversary to degrade the services of the network as well as functionality and performance of network.

In this paper we have proposed a mechanism based on clustering and cryptography which is capable of detecting and defending the DoS attacks. Sensor nodes often use batteries as its power supply, in order to maximize the life time of the WSN and to face the challenges like scalability, fault-tolerance and robustness; an adequate strategy is by grouping of sensor nodes into "clusters". Clustering of sensor nodes provides two major advantages: reduces the complexity of network and intra-cluster coordination which reduces the network traffic by establishing efficient communication schemes. After clustering the WSN, before deployment of nodes each node calculates its original key by using the keys provided by a key distributing server. After deployment, the cluster head authenticates its cluster members that are deployed under it. When a node wants a secure session with another node then both nodes needs to be authenticated in parallel, turn to CH for mutual authentication. If the authentication successful the CH provides a session key to each other which is issued by key distributing server. This key is valid for certain period of time only. After a timeout period the session restarts from the start. The authentication steps are designed very carefully to defend several security breaking DoS attacks.

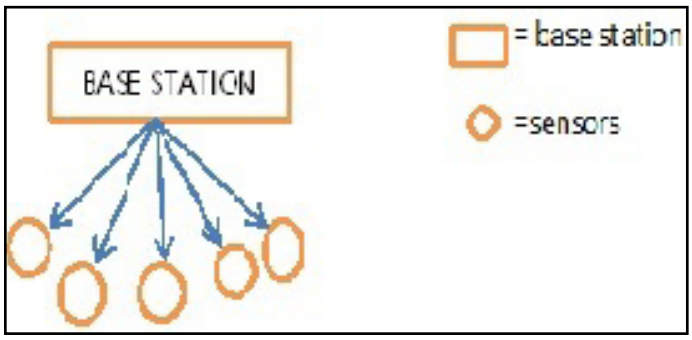

Fig. 1: WSN without clustering

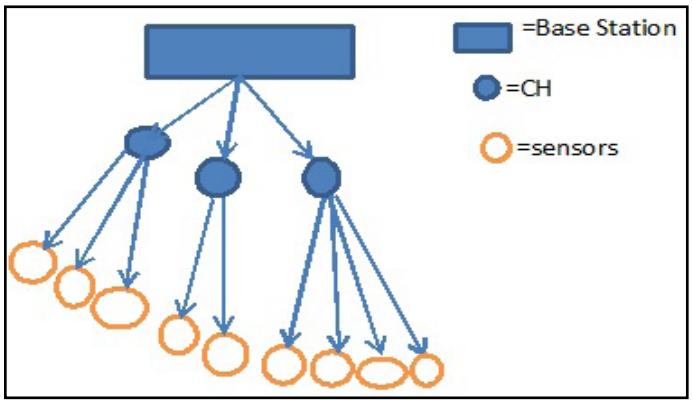

Fig. 2: WSN with clustering

The rest of the paper is organized as follows: Section-II is a brief description about related works on preventing and detecting DoS attacks in WSN. In Section-III we describe how we use

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

the proposed mechanism. In Section-IV we discuss about the simulation results and finally we summarize the conclusion of paper in Section-V.

II. Related Work

In recent times across the world many researchers have developed different types of protocols for preventing DoS attacks and also to safeguard WSN. In paper [1] authors proposed a scheme using game theoretic approach for preventing DoS attacks in WSN. This scheme uses two concepts: utility based source routing which computes the total utility of each source route in data packets. This routing is a dynamic routing mechanism. The other concept is based on a reputation list where each node earns rating from its neighbouring nodes. The disadvantages in this scheme are the node that has less reputation does not get selected in source routing results complexity in routing and difficult to detect compromised nodes if the nodes are large in number. The scheme proposed in paper [2] is a flexible novel framework for detection of denial of service attacks. This is a hierarchal framework consists of two important stages: attacks detection stage and the other is defending stage where various defensive methods are utilised to overcome detected attacks. By this scheme only flooding, jamming, and exhaustion attacks can be detected. The authors in paper [3] proposed a watchdog scheme that detects the misbehaviour nodes and is achieved by using two concepts: watchdog and a path-rater. In the network, every node implements a watchdog which constantly monitors the activities of packet forwarding of their neighbours. The path-rater rates the reliability of transmission of all the alternative routes to a destination node. The disadvantages of this proposed mechanism are that it is not practical for any general routing protocols rather than source routing protocol and the problem of collusion among the compromised or malicious nodes remains unsolved. In paper [4] proposed a novel RSA based framework to prevent the DoS attacks ensures that the malicious nodes prior to the counterparts exhausts the resources. The scheme presented three methodologies to establish an ephemeral key. In [5] for distributed wireless sensor networks (WSN) a scheme is proposed that prevents the possible DoS attacks whenever a packet be intercepted by using a broadcast- key management mechanism. A number of numerical calculations and hashing operations are there to invalidate the first intercepted packet. The Public key cryptography (PKC) technique in [6] prevents only certain DoS attacks which targets on the energy of batteries in WSN. The proposed scheme is a combination of Elliptic curve cryptography (ECC) based key generation and DoS mitigation scheme. A novel cluster based intrusion detection and prevention technique is proposed in [7] to prevent DoS attacks mainly misdirection attacks. The technique builds the clusters from mobile nodes that are in communication range with each other. Among these a node is elected as cluster head (CH) based on two things: fairness-probability of a node as a CH should be equal and efficiency- a node having high efficiency should be selected periodically from the cluster. The authors in paper [8] designed a novel Message Observation Mechanism (MoM) for preventing DoS attacks. This mechanism utilizes similarity function which is based on spatio temporal correlation for identifying the frequency attacks and content attacks. To isolate the compromised or malicious nodes the MoM adopts the reroute and rekeys counter measures. The analysis shows that this solution reduces the energy consumption but detects and defends the DoS attacks.

Table.1 Advantages and disadvantages in related work

Proposed method in	Disadvantages	Advantages
[1]	the node that has less reputation does not get selected in source routing results complexity in routing and difficult to detect compromised nodes if the nodes are large in number	Dynamic routing mechanism
[2]	only flooding, jamming, and exhaustion attacks can be detected	Can maps the flooding, jamming and exhaustion affected areas exactly
[3]	it is not practical to any general routing protocol, only for source routing protocol	Identifies the malicious nodes and avoid them in communication links
[5]	A number of calculations and hashing operations are to be performed to prevent DoS attacks	Prevents the possible DoS attacks by using a broadcast- key management mechanism.
[7]	Detects only misdirection attacks	Can maps the misdirection attacks affected area exactly
[8]	Doesn't give all mechanisms of reroute and rekeys	spatio temporal correlation for identifying the frequency attacks and content attacks. MoM adopts the reroute and rekeys counter measures.

III. Proposed Work

Wireless sensor networks are susceptible to many types of attacks like node replication, capture nodes. These attacks are made by malicious nodes from several sources by using flooding network technique, sends large number of messages to its neighbors or to the base station. In literature several solutions have been proposed to secure the vulnerable wireless sensor networks from these attacks. We believe that the use of clustering and cryptography increases the probability of detecting DoS attacks in WSN. Clustering is mainly useful in applications which require efficient utilization of resources, data aggregation and load balancing. The proposed protocol in [9] called Hybrid Energy-Efficient Distributed clustering (HEED) protocol is used for clustering of sensor nodes. HEED can prolong the network lifetime, produces well distributed control heads (CH), minimizes control overhead and terminates the process of clustering within constant number of iterations.

The network model we considered is divided into clusters, a base station and a key distributing server (KDS). Further, clusters have two types of nodes: Cluster Heads (CH) and Cluster members or sensor nodes. The base station controls the cluster heads, the KDS provides the session keys and unique ids for each node over the network and the cluster heads are responsible to control the intracluster coordination, intercluster communication, cluster server communication and also to coordinate the cluster members within their clusters. In clustering, the essential operation is to select CHs' from the network and then form the clusters from the remaining sensor nodes with these CHs. In HEED, the selection of CHs based on two clustering parameters: 1) residual energy of each node (used to calculate the probability of becoming a cluster head). 2) intra cluster communication cost which is a function of node degree or cluster density. The primary parameter is used to select an initial set of cluster heads probabilistically and the secondary parameter is used to break ties. Each sensor node calculates CHprob the probability of becoming a CH as in [9]. This value should be greater than minimum threshold. If the CHprob value is 1, the node is elected as CH and the node can be tentative CH if its value is less than 1. HEED prolongs the network lifetime than LEACH [10].This is because in LEACH the CH is elected randomly. If the node energy is less might results in faster death but this is avoided in our protocol because the CHs are selected in such a way that their communication cost is minimized and are well distributed over the network. In this paper we are using HEED protocol which is efficient of changing the cluster head after certain iterations which makes the network more reliable. The pseudo code of HEED algorithm is as follows:

A. Initialize

1. S_{nbr} ← {v: v lies within my cluster range}
2. Compute and broadcast cost to $\in S_{nbr}$
3. CHprob ← max (Cprob * (Eresidual/Pmin))
4. is final CH ← FALSE

B. Repeat

1. If ((S_{CH} ← {v: v is a cluster head})=6 φ)
2. My cluster head← leastcost(S_{CH})
3. If(my cluster head=nodeIDN)
4. If(CHprob=1)
5. Cluster head msg (nodeIDN,finalCH,cost)
6. Is finalCH←true
7. Else
8. Cluster $_{head}$ msg (node IDN, tentative CH, cost)
9. Else if (CHprob=1)
10. Cluster head msg (nodeIDN, final CH, cost)
11. Isfinal CH← true
12. Else if random (0,1)<=CHprob
13. Cluster head msg(node IDN, tentative CH, cost)
14. $CH_{previous}$← CHprob
15. CH_{prob}←min (CHprob*2,1)
    Until CHprevious=1

C. Finalize

1. If (is final CH = FALSE)
2. If ((S_{CH}← {v; v is a final cluster head}) =6Ø
3. Myclusterhead← leastcost (S_{CH})
4. Joincluster (cluster head IDN, Node IDN)
5. Else
Cluster head msg (Node IDN, final CH, cost)
6. Else
Cluster head msg (NodeIDN, final CH, cost)

Table 2. Notations in HEED

Notations	Description
Snbr	Probability of sensor node
CHprob	Cluster head probability
Tentative CH	Tentative Cluster Head
Eresidual	Residual Energy
CH	Cluster head
Sch	Selected cluster head
Final CH	Final cluster head
Node IDN	Node identification number
CH previous	Cluster head previous

After clustering the WSN, before deployment of nodes each node sets up a secret special key (K_s) and unique id (ID_i) with the KDS.

A. Calculation of Original Key

To calculate the original key K each node is associated with a pseudo random function (F) [11]. The key can be represented as $K = F (K_s, ID_i)$

B. Mutual Authentication

After deployment, the cluster head authenticates its cluster members that are deployed under it. The cluster head computes a value AC_{ij} based on authentication model proposed in [11] which is represented as

$AC_{ij} = H (ID_i || T_i)$

where H represents Hash function, i represents the CH, j represents the cluster member to authenticate, T_i represents the current timestamp of CH i and ID_i is the unique id of CH. The CH node i sends (AC_{ij}, T_i) to cluster member j. This j node receives the message and checks for the validity of timestamp $(T_j - T_i) \leq \Delta T$ where T_j is current timestamp of cluster member j, ΔT is expected time interval in transmission delay. If this is not satisfied then it denotes that the node j has failed in mutual authentication. Then the CH_i came to know that cluster member j is a compromised sensor node and isolates it from communication. If the above condition is satisfied then the cluster member j computes

$AC_{ji} = H (ID_i || T_j)$

where T_j is current timestamp of node j. Now the sensor node j compares the value AC_{ji} with the received AC_{ij} value. If both values are equal $AC_{ji} = AC_{ij}$ then CHi knows that j node is successfully authenticated. Now it can establish a key safely with this cluster member j. Similarly the cluster heads are authenticated by the server.

C. Establishing Communication in Network

The data that is sensed by the cluster members is sent to the CHs first but not directly to the base station by cluster members and the CH to KDS and this to the base station which results in security from the malicious nodes. After the completion of mutual authentication of every node in the network then the KDS assigns a separate session key (K_{ss}) [12] for each cluster pairs to communicate with it. For this CH and KDS communication, the

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

key can be calculated as

$K_{kds-ci} = H (K_{ss} || ID_i)$

where kds stands for KDS and C_i is a particular cluster, IDi is CH id. This session key is valid for certain period of time T_{ss} only [12]. After this T_{ss} the key gets deleted and the CH become keyless. Again the CH again requests KDS for a new session key. The KDS again performs authentication process and assigns a session key to the requested CH. After distributing the key, KDS immediately sets the validity period of key against its clock pulse. The KDS sends to all CHs in encrypted form about the IDs of all cluster members using its respective session key K_{ss} as

$E_{kds-ci} = (M||ID_{cm})$

Where M represents a message for CHs and ID_{cm} represents the IDs of all cluster members. If a node wants a secure session with another node then node1 sends request to node2 and if node2 accepts the request then both nodes needs to be authenticated in parallel, turn to CH for mutual authentication. If the authentication successful the CH provides K_{ss} to each other. This key is also valid for T_{ss} only. After the time out period the procedure is iterated. This CH and cluster member key can be calculated as

$K_{ci-sk} = H (K_{ss} || ID_i)$

Here C_i represent the CH and S_k represent the corresponding cluster member. Since cluster members reports to a particular CH then the cumulative ID of all cluster members corresponds to the ID of a CH. Now each cluster head can communicate with its cluster members in encrypted way as

$E_{ci-sk} = (M||ID_k)$

which represents that ith CH communicates with k^{th} cluster member. This cluster member decrypts the message using the K_{ss}.

D. Inter-Cluster Communication

Sometimes it may require that if a CH_1 of one cluster wants to communicate with other CH_2 in another cluster then the CH_1 sends a request to CH_2, if its accepts then CH_2 sends its session key K_{ss}^1 to CH_1 and establishes communication which is given as

$K_{ci-cj} = H (K_{ss}^1 || ID_j)$

Where C_i denotes CH_2 and C_j denotes CH_1. The KDS authenticates both nodes before establishing communication. It is the responsibility of CHs to get new session keys after every T_{ss}.

E. Prevention of DoS attacks

When a CH detects a malicious or compromised node during the above processes then it blocks that node from communication with other nodes. Then the cluster head requests the KDS to disrupt the operations of a compromised or malicious node. The KDS simply deletes the secret key of that node from KDS records which results in keyless node. The CH sends the KDS an encrypted message about the malicious node as

$E_{ci-kds} = (ID_i||IP_A||BLOCK)$

Here ID_i represents the ID of the cluster head in which malicious node is detected; IP_A represents the IP address of the malicious node to which services are to be cancelled and to block the detected node for future requests. Further using the proposed Inter-cluster communication method the CHs send an encrypted message to all other cluster heads about the detected malicious node to block it for inter cluster communication as

$E_{ci-cj} = (IP_A||BLOCK)$

where C_i represents the CH in which malicious node is detected and C_j represents the jth CH. Suppose if an attacker launches attacks on the server which consumes the resources of server. As each and every server contains limited number of resources the attack makes the server unavailable to its clients such that it cannot provide services to them whenever it request. This makes the server to reset the network. For this the server broadcast an encrypted message to all CHs as

$E_{kds-ci} = (ID_i||IP_A)$

where ID_i is the unique id of i^{th} CH and the IP address of attacked node to block. Further it is the responsibility of CHs to decrypt the message using its corresponding K_{ss} and to block the malicious node using above communication methods between CHs and cluster members. If the attacker knows our mechanism then only that cluster can be malicious. The remaining clusters do not be disrupted from its operations.

F. Algorithm for the proposed mechanism

- Step-1: Key Distributing Server (KDS) distributes a special key K_s and a unique id ID to each node in the network.
- Step-2: Each node computes its original key using the pseudo random function, special key K_s and unique id.
- Step-3: Checking mutual authentication between server and cluster heads and then cluster heads and cluster members.
- Step-4: Calculate separate session keys K_{ss} for each CH providing communication between server and cluster heads and also between CHs and cluster members.
- Step-5: Using these session keys KDS sends the list of all cluster members to each CH.
- Step-6: The cluster members that belong to a particular cluster can communicate with each other using their respective calculated keys.
- Step-7: The session key valid for T_{ss}. After the time out period the mechanism is iterated that is KDS provides new session keys.
- Step-8: if any adversary performs DoS attacks then execute the Prevention of DoS attacks mechanism.

V. Simulation Results

The simulation results of the clustering technique in [9] shows the performance on network applications as shown below

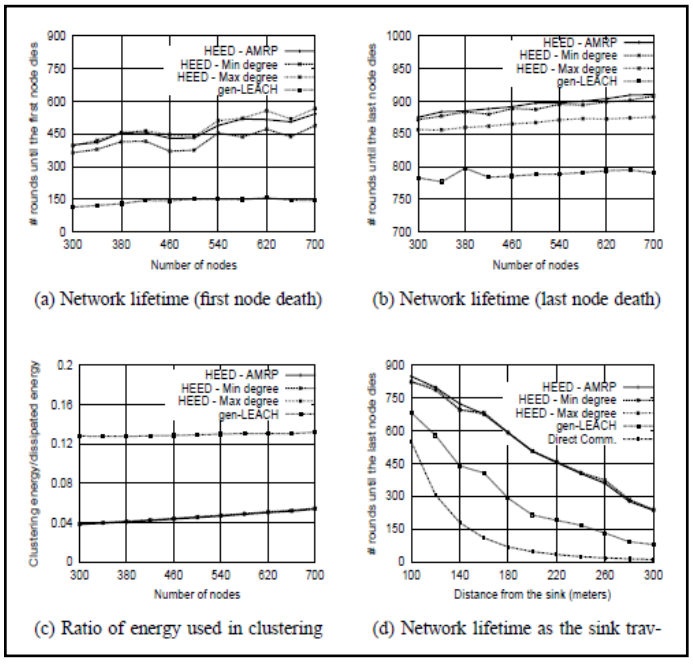

Fig. 3: Performance of HEED protocol on network applications

The authors measures the energy consumed in clusters as a fraction of total dissipated energy in the network. In the above fig. (a) and (b) Compares the network lifetime with HEED in first and last node deaths. In fig (c) illustrates the energy ratio for different number of nodes where HEED expends less energy in clustering. In Fig.(d) it shows that HEED protocol prolongs network lifetime LEACH. Our simulation results shows that the proposed cryptographic mechanism for preventing DoS attacks not only defends the wireless sensor network against them but also maintains integrity, authenticity and confidentiality between sensor nodes. The use of various keys from random function and session keys from KDS plays an important role to combat all kinds of DoS attacks by an adversary. Even if a cluster member is compromised, an adversary cannot gain valuable information from the nodes or server because of the usage of different keys for different purposes. When comparing to the other techniques this technique achieves higher efficiency and accuracy.

V. Conclusion

In this paper we introduced an incorporated cryptographic mechanism and clustering method for preventing DoS attacks energy in WSN's which guarantees that protecting the network from ordinary nodes and also the server from DoS attacks. This scheme retains high security as strong as conventional PKC based broadcast authentication schemes. The authentication mechanism guarantees that all the sensors present in the network are genuine. The sequence of actions adopted successfully defends the network from DoS and blocks the attackers. HEED can prolong the network lifetime, produces well distributed control heads (CH), minimizes control overhead and terminates the process of clustering within constant number of iterations. By these two mechanisms our protocol enforces the other, thus making it a flexible protocol. The concept developed can be applied to a wide range of additional security services that are offered in WSN environments.

References

[1] *Afrand Agah, Mehran Asadi and Sajal K, "Preventing of DoS Attacks using Repeated Game Theory", May 2007.*

[2] *Ouyang Xi, Tian Bin, Li Qi, Zhang Jian-yi, Hu Zheng-Ming, Xin Yang,"A Novel Framework of Defense System Agaist DoS attacks in WSN", IEEE 2011.*

[3] *S. Marti, T. Giuli, K. Lai, M. Baker,"Mitigating routing misbehaviour in mobile ad hoc networks", In Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM) 2000.*

[4] *O. Arazi, H. Qi, D. Rose,"A Public Key Cryptographic Method for DoS mitigation in WSN", IEEE 2007.*

[5] *"A new broadcast key management scheme for distributed WSN", 2009*

[6] *"A public key cryptography method for DoS mitigation in WSN", 2007.*

[7] *"A cluster based intrusion detection and prevention technique in misdirection attack inside WSN", 2013*

[8] *"Yi-ying ZHANG, Xiang-zhen L, Yuan-an LIU, "The detection and defence of DoS attack for wireless sensor network", Elsevier Journal of China Universities of Posts and Telecommunications, Vol. 19, Supplement 2, October 2012, pp. 52-56.*

[9] *Ossama Younis, Sonia Fahmy,"HEED Hybrid Energy-Efficient Distributed clustering", 2004.*

[10] *W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks", IEEE Trans. Wireless Comm., Vol. 1, no. 4, pp. 660-670, Oct. 2002.*

[11] *Rohan Nanda, Shobhit Tiwari and Dr.Venkata Krishna P "Secure and Efficient Key Management Scheme for WSN",ICNCS 2011.*

[12] *Sutirtha Sanyal "SPIKE: A Novel Session Key Management Protocol with Time-Varying Secure Cluster Formation inWSN" IEEE International Conference 2013.*