ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

A Survey on Cluster based Secure and Efficient Data Transfer in Wireless Sensor Networks using HEED

D.Himabindu[1] , S.Neeraja[2] , V.Srikanth[3]

Assistant Professor, Dept. of CSE, Pydah College of Engineering & Technology, Visakhapatnam, India[1]

Assistant Professor, Dept. of CSE, Pydah College of Engineering & Technology, Visakhapatnam, India[2]

Associate Professor, Dept. of CSE, Pydah College of Engineering & Technology, Visakhapatnam, India[3]

ABSTRACT : The wireless sensor networks have been considered as a promising method for reliably monitoring both civil and military environments under hazardous or dangerous conditions. WSN has wide processing capacity in which the data transmission plays a vital role. We are enhancing a system to have a better data transmission rate. Based upon the study we found that the transmission of data in the Military [1] is still not highly secure. So our system enhances the security based on the Digital Signature. Initially we group the nodes in the form of cluster [2] and those clusters have the cluster head to access the region. After the formation of the cluster region, need to analyse the mobility, and therefore to process the data transmission. In WSN clusters are formed dynamically. To select different cluster heads in a region according to the amount of energy we are using the HEED, in the existing system EEDC (Energy Efficient Dynamic Clustering) was used. From the security point of view we are using identity based online/offline digital signature. Hence the system will be much more secure than the present strategy.

KEYWORDS *:* Wireless sensor networks, Cluster head, HEED.

I. INTRODUCTION

A Wireless Sensor Network is a self-configuring network of small sensor nodes communicating among themselves using radio signals, and deployed in quantity to sense, monitor and understand the physical world. Wireless Sensor nodes are called motes . A large number of these sensors can be networked in many applications that require unattended operations, hence producing a wireless sensor network (WSN). In fact, the applications of WSNs are quite numerous. For example, WSNs have profound effects on military and civil applications such as target field imaging, intrusion detection, weather monitoring, security and tactical surveillance, distributed computing, detecting ambient conditions such as temperature, movement, sound, light, or the presence of certain objects, inventory control, and disaster management. Deployment of a sensor network in these applications can be in random fashion (e.g., dropped from an airplane in a disaster management application) or manual (e.g., fire alarm sensors in a facility or sensors planted underground for precision agriculture). Creating a network of these sensors can assist rescue operations by locating survivors, identifying risky areas, and making the rescue team more aware of the overall situation in a disaster area.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

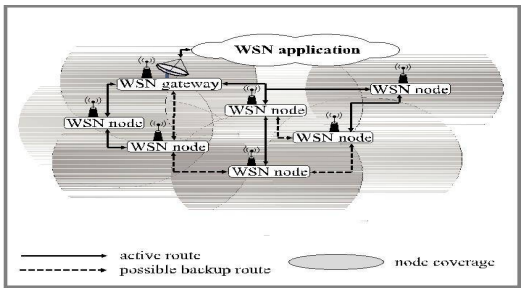

Fig. 1 . Network setup of a typic al wireless adhoc sensor network

Typically, WSNs contain hundreds or thousands of these sensor nodes, and these sensors have the ability to communicate either among each other or directly to an external base station (BS). Sensor nodes coordinate among themselves to produce high-quality information about the physical environment. Each sensor node bases its decisions on its mission, the information it currently has, and its knowledge of its computing, communication, and energy resources. Each of these scattered sensor nodes has the capability to collect and route data either to other sensors or back to an external BS(s). A BS may be a fixed or mobile node capable of connecting the sensor network to an existing communications infrastructure or to the Internet where a user can have access to the reported data. In most applications, sensor nodes are constrained in energy supply and communication bandwidth. Thus, innovative techniques to eliminate energy inefficiencies that shorten the lifetime of the network and efficient use of the limited bandwidth are highly required. Such constraints combined with a typical deployment of large number of sensor nodes pose many challenges to the design and management of WSNs and necessitate energy-awareness at all layers of the networking protocol stack. For example, at the network layer, it is highly desirable to find methods for energy-efficient route discovery and relaying of data from the sensor nodes to the BS so that the lifetime of the network is maximized.

II. RELATED WORK

One of the major threats in wireless sensor network is security and huge consumption of energy which has to be addressed. Energy consumption can be constrained through clustering. Clustering is an effective way of avoiding complexities between sensor nodes of a network which will transmit data to the base station through the cluster head. Digital Signature technique is used to provide security for wireless sensor network which is a critical security service offered in asymmetric key management. As we have introduced clustering technique, our network becomes a “cluster based wireless sensor network”. Dynamic clustering of the sensor nodes will help in reducing the energy consumption to an extent by multi-hop [3] technique.

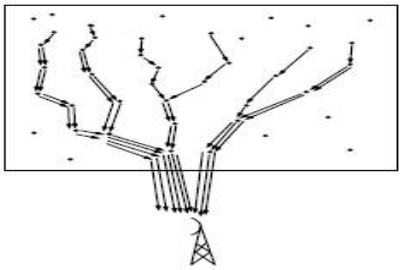

Fig 2 a. Multi-hop without clustering

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

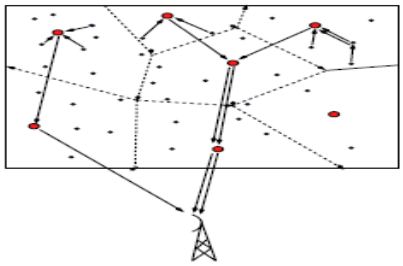

Fig 2 b. Multi-hop with Clustering.

HEED [4] algorithm is used for efficient clustering. HEED (Hybrid Energy-Efficient Distributed clustering), that periodically selects cluster heads according to a hybrid of the node residual energy and a secondary parameter, such as node proximity to its neighbours or node degree. HEED terminates in O(1) iterations, incurs low message overhead, and achieves fairly uniform cluster head distribution across the network. HEED has four primary objectives (i) prolonging network lifetime by distributing energy consumption (ii) terminating the clustering process within a constant number of iterations, (iii) minimizing control overhead (to be linear in the number of nodes), and (iv) producing well-distributed cluster heads. We find that clustering plays a dominant role in delaying the first node death, while aggregation plays a dominant role in delaying the last node death. In each cluster one node acts as a cluster head which is in charge of coordinating with other cluster heads. To increase energy efficiency and prolong network life time we can consider intra cluster communication cost as a secondary clustering parameter. Intra clustering communication involves communicating with other cluster heads. Cost is a function of cluster properties and whether power levels are permissible for transmission with in a cluster. Advantages of HEED are : (i) extends the lifetime of the nodes with in the network .(ii) does not require special node capabilities, such as location awareness (iii) does not make assumptions about node distribution (iv) operates correctly even when nodes are not synchronized. (v) require local information to form the clusters.

I. Initialize

1. $S_{nbr} \leftarrow$ *{v: v lies within my cluster range}*
2. *Compute and broadcast cost to* ϵS_{nbr}
3. $CH_{prob} \leftarrow max(C_{prob} \; X \; E_{residual} \; / \; E_{max} \, , P_{min})$
4. *is_ final_CH* $\leftarrow$ *FALSE*

II. Repeat

1. *If* $((S_{CH} \leftarrow$ *{v: v is a cluster head}*$)\neq\emptyset)$
2. *my_ cluster_head* $\leftarrow$ *least_cost*(S_{CH})
3. *If (my_cluster_head = NodeID)*
4. *If* $(CH_{prob} = 1)$
5. *Cluster_head_msg(NodeID,final_CH,cost)*
6. *is_final_ CH* $\leftarrow$ *TRUE*
7. *Else*
8. *Cluster_head_msg(NodeID, tentative_CH,cost)*
9. *ElseIf* $(CH_{prob} = 1)$
10. *Cluster_head_msg(NodeID,final_CH,cost)*
11. *is_ final_CH* $\leftarrow$ *TRUE*
12. *ElseIf Random(0,1)* $\leq CH_{prob}$
13. *Cluster_head_msg(NodeID,tentative_CH,cost)*

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

14. $Ch_{previous} \leftarrow CH_{prob}$
15. $Ch_{prob} \leftarrow min(CH_{prob} \times 2, 1)$
Until *CHprevious* = 1
III. Finalize
1. If (is_final_CH = FALSE)
2. If $((S_{CH} \leftarrow \{v: v \text{ is a final cluster head}\}) \neq \emptyset)$
3. my_cluster_head ← least_cost(S_{CH})
4. join_cluster(cluster_head_ID, NodeID)
5. Else Cluster_head_msg(NodeID, final_CH, cost)
6. Else Cluster_head_msg(NodeID, final_CH, cost)

Fig 3 Pseudo code for HEED

In Initialization phase, we discover neighbours with in cluster range, the initial cluster head is calculated as $CH_{prob} = f(E_r/E_{max})$. In the Processing phase, the cluster head v receives some cluster head messages and chooses a head with min cost. If v does not have a cluster head it selects a cluster head with CH_{prob}. Here $CH_{prob}=min(CH_{prob} \text{ x } 2,1)$. This process is repeated until $CH_{previous}$ reaches 1. In Finalize phase, the found cluster head is joined with its cluster, otherwise it selects another cluster head.

III. SECURITY

A wireless sensor network is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions. WSNs are more vulnerable to various attacks due to the nature of wireless communication. Since sensors usually have very constrained resources in terms of computing, communication, memory and battery power providing authenticity in WSN poses different challenges. This requires light weight and power saving cryptographic algorithms to support WSN security. Only symmetric –key cryptographic algorithms are suitable tools for providing security in WSN. Specifically Identity-based cryptography is suitable for WSN. Digital Signatures are among the most basic primitives in cryptography, providing authenticity, integrity and non-repudiation in an asymmetric setting in which each user uses two keys public and private keys. In the Identity based setting, the public key of a user simply is his identity. The corresponding secret key is issued by a trusted key generation centre (KGC), who derives the secret key from a master secret key that only the KGC knows. In order to further reduce the computational cost of signature generation online/offline [5] Signature is preferable in WSN. It performs the signature generation in two phases. The first is performed offline (without knowledge of the message to be signed) and the second phase is performed online.(after knowing the message to be signed). The offline phase is executed at the base station, while the online phase is executed at the node. The IBS algorithm is as follows: Initially it generates a public key and a master key. Using the master key and the prior identity, the private key is extracted. Using the public key an offline signature is generated. Using private key, offline signature and a message, it generates an online signature. The generated online signature is verified for further data transmission.

IV. CONCLUSION

We reviewed an energy efficient distributive clustering algorithm in WSNs where energy is consumed less and proposed IBS for secure data transmission

REFERENCES

[1] Michael Winkler, Klaus-Dieter Tuchs, KesterHugjes and Greame Barday Theretical and practical aspects of military wireless sensor networks.
[2] S.Basagni, " Distributed Clustering Algorithm for AdHoc Networks" , Proceedings of International Symposium on Parallel Architecutures, Algorithms , and Networks, pp.310-315, December 1999 .

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

[3] S.Banerjee, S.Khuller,"A Clustering Scheme for Hierarchical Control in Multi-Hop Wireless Networks", Proceedings of IEEE INFOCOM, Anchorage, pp. 1028-1037, April 2001.

[4] Ossama Younis and Sonia Fahmy, "HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad-hoc Sensor Networks ".

[5] Joseph K. Liu, Joonsang Baek, Jianying Zhou, Yanjiang Yang, Jun Wen Wong, Institute for Infocomm Research, Singapore " Efficient online/offline identity-based signature for wireless sensor network".