Reliable Data Transmission for Cluster-based Wireless Sensor Networks

Omerah Yousuf[#1], Mushtaq Ahmed D.M[#2]

#1 OmerahYousuf,M. Tech, Department of Computer Science and Engineering, AMC Engineering College, Bangalore – 560083, India.

#2 Mushtaq Ahmed D.M, Assistant Prof, Department of Computer Science and Engineering, AMC Engineering College, Bangalore – 560083, India.

ABSTRACT

Reliable data transmission is a critical issue in cluster based WSNs (CWSNs). Reliable data transmission problem needs to be handled in a way that it does not affect the overall performance of the system and at the same time imposing the secure data transmission property as well. The paper aims at imposing the property of secure data transmission in the cluster based Wireless sensor Networks. In this paper we propose a secure and efficient solution for data transmission in Wireless Sensor Networks using two Secure and Efficient data Transmission (SET) protocols – SET-IBS and SET-IBOOS which in turn use Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital signature (IBOOS) scheme, respectively. The key idea is to authenticate the encrypted sensed data by applying digital signatures to message packets and applying the key management for security. Both these proposed protocols i.e. SET-IBS and SET-IBOOS have better performance than the existing secure protocols for CWSNs in terms of security overhead and energy consumption. The proposed system was evaluated in terms of security from the perspective of three types of attacks – passive, active and node compromising. To provide data security during data transmission, we use AES algorithm.

Key Words: Cluster-based WSNs, ID-based digital signature, ID-based online/offline digital signature

Corresponding Author: Omerah Yousuf

INTRODUCTION

A wireless sensor network (WSN) consists 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. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance;

today such networks are used inmany industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

Wireless sensor network is an emerging field where lots of research work has been done involving hardware and system design, networking, security factor and distributed algorithm. Sensor nodes normally sense the data packet and transfer it to the base station via some intermediate nodes. The sensor nodes are low cost, low power and short transmission range [1]. Nodes use to send data packet locally to its single hop neighbor nodes and so on and finally it reaches to its base station. There are basically two types of data transmission in wireless sensor network, these are – direct transmission and multi-hop data transmission. In direct transmission data are sending directly to the sink whereas multi-hop transmission data send via no of intermediate nodes lies between source node and base station. In sensor network the flow of data is very important aspect because each data packet contains the event which may be very important for some application. Thus data transmission must be secured. Basically to make the data transmission secure we have to maintain two basic fields these are – Authentication and confidentiality. Authentication means it has to make sure that data packet comes from the intended sender or packet received by the intended receiver those which are involved in the transmission process. Confidentiality refers preventing the data packets from any unauthorized access. The task of securing wireless sensor networks is however, complicated because sensors are highly anonymous devices with a limited energy and memory capacity, and initially they have no knowledge of their locations in the deployment environment.

Grouping sensor nodes into clusters has been widely investigated by researchers in order to achieve the network system's scalability and management objectives. Every cluster would have a leader sensor node, often referred to as the cluster-head (CH), which can be fixed or variable. CHs aggregate the data collected by the sensor nodes in its cluster, thus, clustering decreases the number of relayed packets. Asthe benefits of clustering, it conserves communication bandwidth and avoids redundant exchange of messages among sensor nodes, because of limiting the inter-cluster interactions. Therefore, clustering prolongs the lifetime of WSNs [2] [3].

Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Many data transmission protocols for WSN including the cluster based are vulnerable to number of security attacks [4]. In cluster based protocols since the data aggregation and routing of data depends on CH.so the attacks to the CH can cause serious damage to the network. If an attacker manages to turn into a CH, it can provoke attacks such as sinkhole and selective forwarding attacks, thus disrupting the network. On the other hand, the attacker may intend to inject bogus sensing data into the network, especially to pretend as leaf nodes sending bogus information towards the CHs [5].

Attacks in Wireless Sensor Networks

Depending upon the attacking means we have three types of attacks in WSN:

• *Passive attack:* The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature. Passive attackers are able to perform eavesdropping at any point in the network or even the whole communication of the network. *Eavesdropping* is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents. When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, the eavesdropping can act effectively against the privacy protection.

• *Active attack:* The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The active attackers can forge, reply and modify messages. Especially in WSNs, various types of active attacks can be triggered by attackers, such as bogus and replayed routing information attack, sinkhole and wormhole attack, selective forwarding attack, HELLO flood attack, and Sybil attack [4] [5].

• *Node compromising attack*: Node compromising attack can physically compromise sensor nodes, by which they can access the secret information stored in the compromised nodes, e.g., the security keys. The attackers also can change the inner state and behaviour of the compromised sensor node.

RELATED WORK

There has been a lot of research done in the area of Cluster-based data transmission security issues carried out by the prominent authors in the recent past. Since it is one of the hot research areas of the 21st century, we can easily find a huge amount of research material on which this paper can be built and the new mechanism which will be efficient than the existing approaches will be proposed.

In the year 2002, AratiManjeshwar, Qing-An Zeng and Dharma P. Agrawal in their paper titled, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using APTEEN Protocol" [6] developed an M/G/1 model to analytically determine the delay incurred in handling various types of queries using enhanced APTEEN (Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network protocol) protocol. This protocol uses an enhanced TDMA schedule to efficiently incorporate query handling, with a queuing mechanism for heavy loads. It also provides the additional flexibility of querying the network through any node in the network to verify the analytical results, simulated a temperature sensing application with a Poisson arrival rate for queries on the network simulator ns-2. As the simulation and analytical results match perfectly well, this can be said to be the first step towards analytically determining the delay characteristics of a wireless sensor network. This analytical model confirms that the delay in answering the queries depends greatly on the frame length. Frame length can be reduced

if all the CHs use different CDMA codes to communicate with the BS. Since BS is not energy constrained, this should not affect the overall performance.In the year 2006, paper titled "A survey of security issues in wireless sensor networks" [4] discussed about the security issues in WSN. This paper discussed about the constraints, security requirements, and attacks with their corresponding countermeasures in WSNs and also presented a holistic view of security issues. These issues are classified into five categories: cryptography, key management, secure routing, secure data aggregation, and intrusion detection. This paper also highlighted the advantages and disadvantages of various WSN security protocols and further compare and evaluate these protocols based on each of these five categories. This paper pointed out the open research issues in each subarea and concluded with possible future research directions on security in WSNs.

In the year 2010, Huang Lu, Jie Li, and Hisao Kameda in their paper titled "A Secure Routing Protocol for Cluster-based Wireless Sensor Networks Using ID-based Digital Signature."[7] discussed about the secure routing for cluster based sensor networks where clusters are formed dynamically and periodically. In this paper the authors pointed out the deficiency in the secure routing protocols with symmetric key pairing. Along with the investigation of ID-based cryptography for security in WSNs, proposed a new secure routing protocol with ID-based signature scheme for cluster-based WSNs, in which the security relies on the hardness of the Diffie-Hellman problem in the random oracle model. However, the simulation results pointed out the issues in the proposed protocol that the extra energy consumption by computation of the auxiliary security overhead is still large.However, the researchers are trying to improve the simulation experiments with other secure routing protocols for better results, and improve the protocol in energy efficiency with pairing.

In the year 2010, RehanaYasmin, Eike Ritter and Guilin Wang in the paper titled, "An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures: Implementation and Evaluation" [8] addresses the problem of authentication in WSN. They proposed an authentication framework for WSNs using Identity (ID) - based Cryptography and Online/Offline Signature (OOS) schemes. This framework is comprised of two authentication schemes; quick authenticated broadcast/multicast by sensor nodes and outside user authentication. The first scheme allows every sensor node in the network to broadcast or multicast authenticated messages very quickly without the involvement of the base station. All potential receivers can verify a message sent by any sender node in the network. It also allows sensor nodes on the path from the sender node to the receivers to verify a valid message and drop false injected data. The second scheme enables all sensor nodes in the network to verify the legitimacy of any outside user without storing any user specific information. It allows a maximum possible number of legitimate users to access data from sensor nodes in a secure way. This scheme first authenticates a user and then establishes a session key for the secure exchange of user queries and sensor nodes data.

The proposed framework uses an ID-based Online/Offline Signature (IBOOS) (an ID-based version of OOS) for the first scheme and an ID-based Signature (IBS) for the second scheme. The authors of this paper assessed the cost incurred by using two different IBOOS schemes for

resource constrained sensor nodes. They first implemented and evaluated one pairing based IBOOS scheme named as XIBOOS. For optimization purposes, also converted the well-known pairing-free BNN-IBS scheme into an IBOOS scheme and implemented it on MICA2 sensor nodes. The implementation results show the suitability of IBOOS for WSNs. However they did not focused on the session key establishment between the outsider user and the sensor node after successful user authentication, i.e., the second authentication scheme of the proposed framework.

PRELIMINARY CONCEPTS

The LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol presented by Heinzelman et al. [9] is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. In order to prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime. Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's clusters and data links. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols. There are some secure data transmission protocols based on LEACH-like protocols, such as SecLEACH [10], GS-LEACH [11] and RLEACH [12]. Most of them, however, apply the symmetric key management for security, which suffers from a so-called orphan node problem[13]. This problem occurs when a node does not share a pairwise key with others in its preloaded key ring, in order to mitigate the storage cost of symmetric keys, and the key ring is not sufficient for the node to share pairwise symmetric keys with all of the nodes in a network. In such a case, it cannot participate in any cluster, and therefore, has to elect itself as a CH. Furthermore, the orphan node problem reducesthe possibility of a node joining a CH, when the number of alive nodes owning pairwise keys decreases after a long-term operation of the network. Since the more CHs elected by them, the more overall energy consumed of the network [9], the orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs. Even in the case that a sensor node does share a pairwise key with a distant CH but not a nearby CH, it requires comparatively high energy to transmit data to the distant CH.

The objective of the reliable data transmission for CWSNs is to guarantee a secure and efficient data transmission between leaf nodes and CHs, as well as transmission between CHs and the BS. The aim of the system is to solve the orphan node problem by using the ID-based crypto-system that guarantees security requirements, and propose SET-IBS by using the IBS scheme. Furthermore, SET-IBOOS is proposed to reduce the computational overhead in SET-IBS with the IBOOS scheme and providing the data security using AES algorithm.

ARCHITECTURAL DESIGN

The architectural design of the system is shown in the **Figure 1**. The system starts with Source initiating the request to send the data. The source will locate and identify all the neighboring

nodes in the network of a particular cluster. All the neighboring nodes are identified with the help of a router connecting the nodes in a particular cluster. After locating the nodes in the system, with the help of router all possible routing paths are found. The particular route is selected and upon the checking of MAC. The route is selected among the different available routing paths based on the number of hops a packet needs to travel before reaching the destination. The path with the minimum number of hops is selected as the routing path.

Also it is worthy here to mention that it is necessary to check the MAC (Message Authentication Code) of the selected path. The message authentication code needs to be checked in order to ensure that an authentic user is sending the packet to an authentic receiver. This issue may be elaborated by means of an example as follows – suppose in an organization the manager needs to send the particular information to some particular employees only. As the information may be confidential one, it must not reach tothose people who can create problems out of this information. So here need to select a particular gateway only to make sure that the information reaches the targeted users only. This is the reason behind checking the MAC before sending the data.

After checking the MAC, the route is verified in order to ensure that the route which has been selected is the real route on which the data packets need to be sent. It is a type of cross check to ensure that the authentication of data is made in reality. Once done with the verification of the route, the route which has been selected is activated in order to carry out the process of communication between the source and the destination nodes via different nodes in the cluster. In other words, actually here it is performing the task of activating the verification in a way that signals the nodes to start communication as the security needed to ensure that the reliable communication has been incorporated. Now are ready to start the communication as the path has been set now.

And finally when done with all the steps in order to ensure that reliable communication occurs between the source and destination nodes, it is needed to send the actual information i.e., "Data"via the established path. Since it is needed to ensure that the data that passes through the secure path established above must also be secure, so "Encrypt" the data and then send it.

The module which deals with the encryption and sending of data makes sure that there are no active attackers present in the cluster. In other words the attackers are being monitored continuously and checked upon by the system. In case the attackers are found in the cluster, it is necessary to perform the task of filtering the attackers and reverting back to the module responsible for encryption and sending of the data, the data is now secure and you are free to execute your action now.

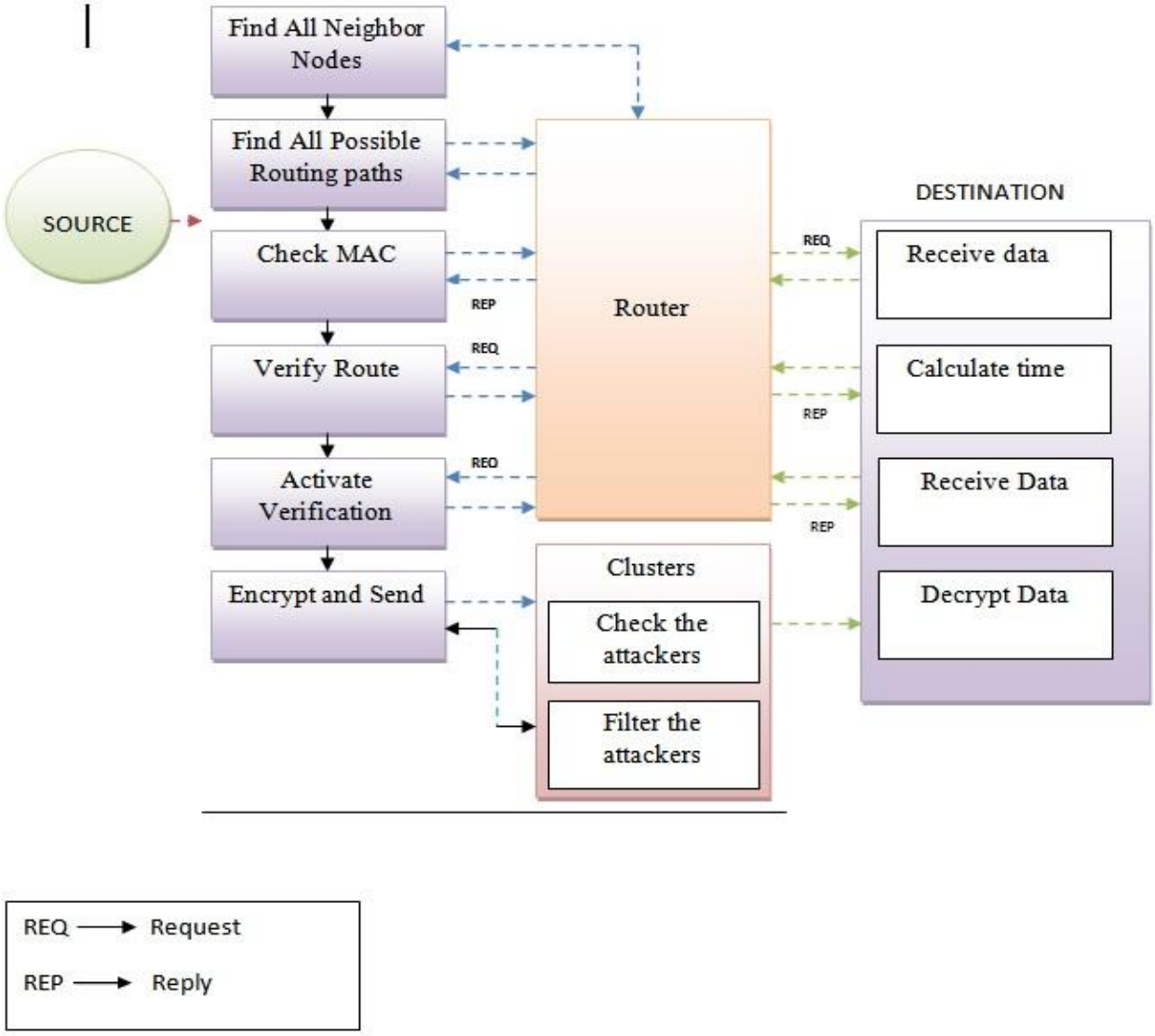

Figure 1: Proposed Architectural Design

It is worth to mention here that the encryption of the data and the filtering of the attackers if present take place in a loop form. It is like checking for a valid signal to go on. Once the encryption module sends the data, it is checked upon for attackers and only after the positive signal from the Filtering Module the sending of data takes place. In this way make sure that the data which is being send is both reliable and secure. And when the data as well as the established communication path is secure, it is surely ensuring the security of the messages in the network and hence the reliability and security of communication in a wireless sensor area network is established, which is the motive behind this paper.

At the **Receiver's** side the data is received and the time that has been taken after the data packet was sent by the source and the time at which the data packet has been received by the receiver is calculated. Once the delay is calculated at the receiver's side, it is replied back to the router in order to make sure that it is using the path with the minimum delay for the purpose of the communication. The router will compare the delay occurred with the existing path delays between the particular source and destination and select the one with the least time delay. In this way the communication is made as "Efficient". Also since the data sent by the source is in Encrypted form, the data is "Decrypted" at the receiver's side in order to obtain the required information sent by the source.In this way the communication between the different nodes in a cluster is made **Secure** as well as **Efficient**.

CONCLUSION

WSN is a challenging and promising system concept and requires new types of architectures and protocols as compared to traditional wired/wireless networks. WSN are used in lot of applications in present day world. Energy is an extremely critical resource for battery-powered WSN. Making energy balanced protocol design a key challenging problem. So incorporation of Energy Efficiency in WSN is need of the hour. For providing energy efficiency in WSN concept of clustering is used and secure data transmission among clusters is very important. To provide the reliable data transmission in CWSNs we propose two SET protocols called SET-IBS and SETIBOOS, by using the IBS scheme and the IBOOS scheme, respectively. We need to make sure that the security is imposed in the system but not at the cost of efficiency. Thus, we need to solve one issue keeping in mind the second one simultaneously. The protocols provide both security as well as efficiency in terms of attacks and data transmission respectively. Thus, we can conclude that the proposed system is both effective in tackling attacks in WSN as well as being an efficient one in terms of data transmission delays.

REFERENCES

[1] Yu Wang, Hongyi Wu, and Nian-FengTzeng ,"Energy-efficient Data Transmission in Wireless Sensor Networks", in Center for Advanced Computer Studies University of Louisiana at Lafayette P.O. Box 44330, Lafayette, LA 70504.

[2] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," Computer Communications, vol. 30, no. 14- 15, 2007.

[3] J. Ibriq and I. Mahgoub, "Cluster-Based Routing in Wireless Sensor Networks: Issues and Challenges," in Proc. of SPECTS'04, 2004.

[4] Y.Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Commun. Surveys Tuts., vol. 8, no. 2, 2006.

[5] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Ad Hoc Networks, vol. 1, no. 2-3, 2003.

[6] A. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, "An analytical model for information retrieval in wireless sensor networks using enhanced APTEEN protocol", IEEE Trans. ParallelDistrib. Syst., vol. 13, 2002.

[7] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based WSNs Using ID-Based Digital Signature," in Proc. IEEE GLOBECOM, 2010.

[8] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures," in Proc. IEEE CIT, 2010.

[9] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," IEEE Trans. WirelessCommun., vol. 1, no. 4, 2002.

[10] L. B. Oliveira, A. Ferreira, M. A. Vilac¸a et al., "SecLEACH-On the security of clustered sensor networks," Signal Process., vol. 87, 2007.

[11] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and performance analysis of a secure clustering protocol for sensor networks," in Proc. IEEE NCA, 2007.

[12] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," in Proc. WiCOM, 2008.

[13] S. Sharma and S. K. Jena, "A survey on secure hierarchical routing protocols in wireless sensor networks," in Proc. ICCCS, 2011.Nokia (2005).