ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
December 2012,
Vol. 5, No. (2):
Pgs. 321-325

Secure Dynamic Data Aggregation Routing Protocol for Wireless Sensor Networks

BHAWANA MATHUR

Asst. Professor ,Sri Balaji Technical Campus,Jaipur

(Received: April 12, 2011; Accepted: June 04, 2011)

ABSTRACT

Routing in sensor networks is complicated due to several issues ranging from security to energy constraints of wireless sensor nodes. This distinguishes them from contemporary wireless ad hoc networks. Adversaries can launch DoS attacks by injecting false data reports via compromised nodes. Previously a Hill Climbing key dissemination filtering scheme was developed where each node disseminates its key to forwarding nodes and later transmits reports along with the key. The forwarding nodes validate the credibility of the reports based on the key obtained earlier. This approach assures stronger filtering capacity for nodes closer to data sources and achieves secure and reliable transmissions. Sensor nodes process capability, bandwidth and battery capacity is still scarce. It is necessary to save resources of sensor nodes with the purpose of prolonging network lifetime. In that regard we propose to use a dynamic data aggregation routing protocol, named DABDR along with the earlier filtering scheme for secure and dynamic transmissions in Wireless Sensor Networks.

Key words: DoS(Denial of Service),Hill Climbing, DABDR (Data Aggregation Based on Dynamic Routing), Wireless sensor networks.

INTRODUCTION

Wireless sensor networks (WSNs)[2] provide a technological basis for many different security-critical applications, such as military surveillance, critical infrastructure protection and surveillance. WSNs can be deployed in unattended and even hostile environments for monitoring the physical world. The monitored environment is covered by hundreds or even thousands of sensor nodes with embedded sensing, computation, and wireless communication capabilities. The resources of these sensor nodes are very constrained because sensor nodes are mostly cheap and battery-powered.

As a result of the low cost nature of WSNs, sensor nodes are (mostly) not tamper-resistant and can be easily compromised by an adversary. The entire information (e.g., keying material) stored on the nodes can therefore be misused by the adversary to act as authorized nodes in the network. As a result an adversary can perform insider attacks such as false data injection, e.g., indicating a non-existing event to cause false alarms, or Path-based Denial of Service (PDoS) attacks. In a PDoS attack, an adversary overwhelms sensor nodes by flooding a multihop end-to-end communication path with either replayed or injected false messages to waste the scarce energy resources.

A dynamic en-route filtering scheme to address both false report injection attacks and DoS attacks in wireless sensor networks. In this scheme, sensor nodes are organized into clusters. Each legitimate report should be validated by multiple message authentication codes (MACs), which are produced by sensing nodes using their own authentication keys. The authentication keys of each node are created from a hash chain. Before sending reports, nodes disseminate their keys to forwarding nodes using *Hill Climbing* approach. Then, they send reports in rounds. In each round, every sensing node endorses its reports using a new key and then discloses the key to forwarding nodes. Using the disseminated and disclosed keys, the forwarding nodes can validate the reports. Recently, technologies have developed rapidly. However, with the limitation of costs and size, the process capability, bandwidth and battery capacity of sensor nodes is still small. Especially, in many applications, sensor nodes are deployed in unreachable environments so that it is difficult to supplement battery capacity. Therefore, it is necessary to consider how to save resources of sensor nodes with the purpose of prolonging network lifetime.

Data aggregation is defined as the process of aggregating the data from multiple sensors to eliminate redundant transmission and provide fused information to the base station. Data aggregation usually involves the fusion of data from multiple sensor nodes at intermediate nodes and transmission of the aggregated data to the base station. Data aggregation attempts to collect the most critical data from the sensors and make it available to the sink in an energy efficient manner with minimum data latency.

Most of the routing schemes in present data aggregation protocols are static, that is, how data will flow to sink is determined before data being collected. Data aggregation has been proposed as one method for reducing energy consumption in sensor networks. One critical factor in data aggregation is routing. There is a data aggregation protocol based on dynamic routing named DABDR, is proposed, to make data aggregation more efficient. we have proposed how to reduce delay and overhead and also try to make sure whether all data have been aggregated or not, to make data aggregation more efficient. The dynamic routing in DABDR is based on two potential field: Depth potential field is to make packets flowing to sink and DA queue length potential field is to make packets more concentrated in spate and thus data aggregation will be more efficient.

Related Work

Routing schemes in present data aggregation protocols are static, that is, how data will flow to sink is determined before data being collected. Present data aggregation protocols mainly based on three kinds of routing schemes which respectively organize sensor networks into clusters, a chain or a tree. Cluster-based data aggregation protocols organize sensor nodes into clusters, a Chain, a tree.

Cluster has a designated sensor node as the cluster head which aggregates data from all the sensors in the cluster and transmits the concise digest to the sink. The typical examples are LEACH [6] and HEED [17]. The distinct of these two protocols are the method of selecting cluster heads. LEACH assumes all the nodes have same amount of energy capacity in each election round. The main goal of HEED is to form efficient clusters for maximizing network lifetime. Cluster –head selection is based on a combination of node residual energy of each node and a secondary parameter which depends on the node proximity to its neighbors or node degree [4]. Compared with the scheme that all the sensor nodes directly transmit all the data to sink, cluster-based data aggregation protocols reduce the amount of information that is transmitted to the sink and thus save energy [4,7]. One disadvantage of cluster-based data aggregation protocols is that if sensor nodes are far away from their cluster head, they might expend excessive energy in communication. Further improvements in energy efficiency can be obtained if sensors transmit only to close neighbors. Chain-based data aggregation protocols organize sensor nodes as a chain along which data flow to sink. The key idea behind chain-based data aggregation is that each node transmits only to its closest neighbor. The chain can be constructed by employing a greedy algorithm or the sink can determine the chain in a centralized manner. Greedy chain formation assumes that all nodes

have global knowledge of the network. A typical chain-based data aggregation protocol PEGASIS employ the greedy algorithm to construct the chain. The distances that most of the nodes transmit are much less compared to LEACH, in which nodes transmit to its cluster head. Hence, PEGASIS protocol has considerable energy savings compared to LEACH[4].

Tree-based data aggregation protocols organize sensor nodes into a tree where data aggregation is performed at intermediate nodes along the tree and a concise representation of the data is transmitted to the root node which is usually the sink. One of the main aspects of tree-based networks is the construction of an energy efficient data-aggregation tree.

Hill Climbing

Important observations of hill climbing are: First, when multiple clusters disseminate keys at the same time, some forwarding nodes need to store the auth-keys of different clusters. *The nodes closer to the base station need to store more auth-keys than others (typically those closer to clusters) do* because they are usually the hot spots and have to serve more clusters. Second, *the false reports are mainly filtered by the nodes closer to clusters, while most nodes closer to the base station have no chance to use the auth-keys they stored for filtering*. If we could let the nodes closer to clusters hold more auth-keys, the false reports can be dropped earlier. Therefore, to balance the memory requirement of nodes and provide a higher filtering capacity, we propose *Hill Climbing* approach, which achieves that the nodes closer to clusters hold more auth-keys than those closer to the base station do. *Hill Climbing* involves two variations, one for the key predistribution phase and the other for the key dissemination phase.

Hill Climbing has two advantages

1) It makes the upstream nodes get more auth-keys than not only the downstream nodes but also other upstream nodes at the same positions without using *Hill Climbing*.
2) It eliminates redundant decryptions and verifications because if an auth-key has been decrypted by an upstream node, any downstream node no longer needs to decrypt the key (or use it to verify reports).

DABDR: Dynamic Routing Based On Data Aggregation

Data aggregation based on dynamic routing is sampled in Fig.1. Green arrows represent the possible path if employing present tree-based data aggregation protocols. Data generated at flow to sink along the orange arrow is anticipated.

As shown in Fig.1, if routing scheme just selects a minimum path in terms of distance, then data generated at region 1 and region 2 will flow to sink along two different offsets of the routing tree.

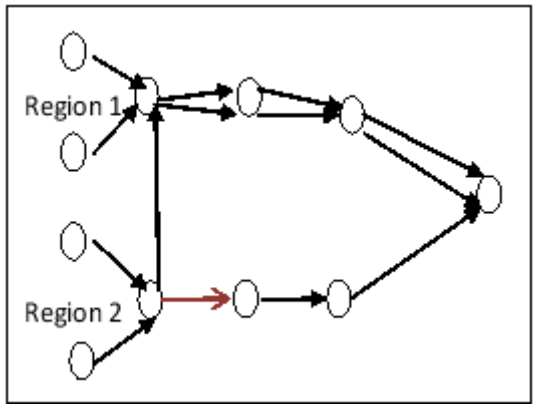

Fig. 1. Data aggregation on DABDR

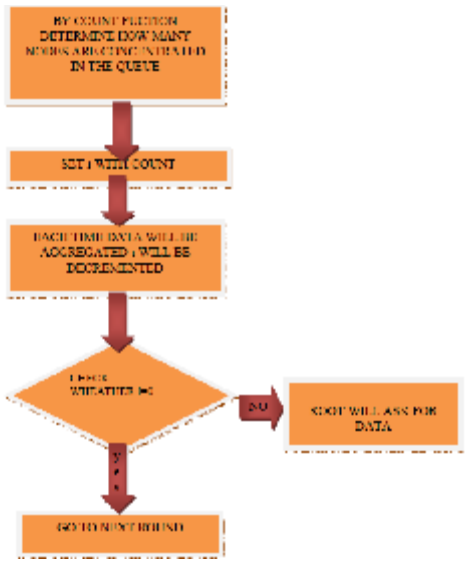

Fig. 2. Flowchart on approach 2

But if data generated at region 2 flow along the orange arrows, data aggregation will be more efficient in terms of total energy consumption of the sensor network. To achieve this, node needs to know some dynamic information in the process of data flowing to sink

Periodic synchronization algorithms for data aggregation can be classified into two approaches as discussed below. Periodic simple aggregation means that each node waits a predetermined amount of time, aggregates all data received, and then forwards the data toward the host node. Such an algorithm is simple to implement, but does not guarantee accuracy of the data. Periodic per-hop aggregation means that each node waits until it receives data from all children, aggregates the data, and then forwards it toward the host node.

Approach 1

Solution on DABDR, if any node can fail to send data. Steps for this approach are given below:

- Start
- Each node stores previous record and also a threshold would be included with each query (threshold determines how much change needs to happen to report)
- Sense current reading
- If any change more than threshold then it reports otherwise doesn't report.
- If a node doesn't report then the parent stores last reported value of it
- The parent calculates the average of the values of the nodes and send to its parent and thus finally to host
- Then the host sends the final average value to the children by which the threshold is determined.
- End.

We want to ensure every node holds that value which is required. So only one report is required for that. So if any node fails, another node will be involved until reporting. Besides sensing own data nodes will also try to listen data of the neighbors. According to the function, the node will update its data with that. Here we only considered max, min value for data aggregation of dynamic routing, if any node fails to send data.

Approach 2

Solution on DABDR of all data have been aggregated. Steps for this approach:

- Start
- By count function determine how many nodes are concentrated in queue
- Initialize i with count
- Each time data will be aggregated i will be decremented.
- If i=0 reporting finished go to next round
- If i! =0 not all data have been aggregated again ask for data
- End.

This DABDR technique only assumes that all data have been aggregated. To make confirmation whether all data have been aggregated.

Performance

Our Approach 1 mainly focuses on getting max, min or median value. Sometimes many nodes fail to send data due to various reasons. May be nodes can die or any other reason. But the data maybe important for this if only max, min or median value is required all nodes can hold only the required data and any node can report that not involving all nodes and it only requires to report once. If once reported not to spend any more time for that data. Thus it solves network traffic, delay and also makes it more energy efficient.

Our third algorithm focuses on queue to make sure all data are aggregated in the queue for which we have raised an algorithm which will make confirmation whether all data has been reported or not.

CONCLUSION

Routing in sensor networks is a new area of research, with a limited, but rapidly growing set of research results. In this paper, we presented a comprehensive survey of routing techniques in wireless sensor networks which have been presented in the literature. They have the common objective of trying to extend the lifetime of the sensor network, while not compromising data delivery.

In this paper, a dynamic en-route quarantine scheme for filtering false data injection attacks and DoS attacks in wireless sensor networks. In our scheme, each node uses its own auth-keys to authenticate their reports and a legitimate report should be endorsed by nodes. The authentication keys of each node are created from a hash chain. Before sending reports, nodes disseminate their keys to forwarding nodes using *Hill Climbing* approach. Here, Data aggregation has been proposed as one method for reducing energy consumption in sensor networks. To prolong the network life time, we propose to use a dynamic data aggregation routing protocol, named DABDR along with the earlier filtering scheme for secure and dynamic transmissions in Wireless Sensor Networks. The proposed protocol will reduce delay and overhead and also try to make sure whether all data have been aggregated or not, to make data aggregation more efficient.

REFERENCES

1. Mohamed Watfa , William Daher and Hisham Al Azar, A Sensor Network Data Aggregation Technique.
2. Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, A Survey on Sensor Networks Georgia Institute of Technology
3. Rajashree.V.Biradar (1) , V.C .Patil (2) , Dr. S. R. Sawant (3) , Dr. R. R. Mudholkar , Classification And Comparison Of Routing Protocols In Wireless Sensor Networks Special Issue on Ubiquitous Computing Security Systems, *UbiCC Journal* – 4
4. Jamal N. Al-Karaki Ahmed E. Kamal, Routing Techniques in Wireless Sensor Networks: A Survey ISSN: 2249-1945 *NagaLakshmi et al*, GJCAT, **2**(1): 1024-1028 1028 (2012).
5. L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. ACM CCS*, 41–47 (2002).
6. Zhang Jiao, Ren Fengyuan, He Tao, Lin Chuang, Data Aggregation Protocol Based on Dynamic Routing in Wireless Sensor Networks,
7. O. Younis and S. Fahmy, "HEED: a Hybrid, Energy Efficient, Distributed Clustering Approach for Ad Hoc Sensor networks,"IEEE Trans. Mobile Computing, **3**(4) 366–79 (2004).
8. Ramesh Rajagopalan and Pramod K. Varshney, Data aggregation techniques in sensor networks: A survey .
9. R. Jurdak, C. V. Lopes, P. Baldiy, A Framework for Modeling Sensor Networks, 19th Annual ACM Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA'04), (2004).
10. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, Energy-Efficient Communication Protocol for Wireless Microsensor Networks, IEEE Proceedings of the IEEE International Conference on System Sciences, (2000).
11. Bhaskar Krishnamachari, Deborah Estrin, Stephen Wicker, The Impact of Data Aggregation in Wireless Sensor Networks.
12. *NagaLakshmi et al*, GJCAT, 2 (1), 1024-1028 1028 [5] (2012).