Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg. 374 – 380

RESEARCH ARTICLE

ENERGY EFFICIENT VOTING BASED INTRUSION DETECTION TECHNIQUES IN HETEROGENEOUS WIRELESS SENSOR NETWORK

Divya.B[1], Manju.R[2], Sathyabama.B[3]

[1,2,3] V.S.B Engineering College affiliated to Anna University, Karur

[1] divyaccet@gmail.com, [2] manjususila@gmail.com, [3] sathyadharshana@gmail.com

Abstract: ***In this paper a lot of extensions of malicious attacks for packet dropping and bad mouthing attacks with implications to energy, reliability and security. Multipath routing based tolerance protocols and intrusion detection are utilized in these attacks. Light weight intrusion detection system is used to detect malicious nodes in networks and to decrease the energy loss, increase the QoS and achieving high security and Trust/reputation management system to investigate Strengthen intrusion detection through "weighted voting" and provides the trust system for neighbor nodes as well as to overcome the downside in multipath routing for intrusion tolerance in WSNs for achieving high security and utilizing the HWSNs time period.***

Index Terms: Intrusion detection; multipath routing; Trust system; Cluster head; Heterogeneous wireless sensor networks

I. INTRODUCTION

A Wireless sensor network (WSNs) consist of autonomous sensors to observe environmental conditions like temperature, sound, vibration, pressure and pass their data through the network to main location.SNs are used for sensing the environment are used to read the sensing information and transmit to base station and also used for monitoring purposes Sensor node is a tiny device includes three basic components: 1) A sensing subsystem for data acquisition from physical surrounding environment processing subsystem for local data processing and storage, and Wireless communication subsystem for data transmission, processing and storage, and a wireless communication subsystem for data transmission.2) A power source is used to supply the energy needed by the device to perform the programmed task and power source is often consists of a battery with a limited energy budget. 3) SNs are

battery-powered devices, the critical aspect to face concern how to reduce the consumption of energy for all nodes, so that the lifetime of network can be extended to a reasonable timesbudget.3) SNs are battery-powered devices, the critical aspect to face concern how to reduce the consumption of energy for all nodes, so that the lifetime of network can be extended to a reasonable times.

The tradeoff Performance of both energy consumption and QoS gain in both security and reliability to maximize the system lifetime and also uses the multipath routing to tolerate intrusion detection process where decision is based on a majority voting of monitoring nodes and considering energy being consumed for intrusion detection. Both cluster head (CHs) and sensor nodes (SNs) can be compromised for lifetime maximization. The basic idea is that heterogeneous wireless sensor network (HWSNs) nodes having wireless link with dissimilar communication range, sensing range, densities and capabilities. It Increases the network lifetime and reliability and energy also achieved.

Intrusion detection system (IDS) is used to detect malicious nodes. Two problems will arise:1)what paths to use and 2) how many paths to use and to overcome this problem multipath routing is used, is a routing technique of using multiple alternative paths through a network. Trust based systems are used to tackle the "what path to use" problem and here trust based intrusion detection observe the existence of optimal trust threshold for minimizing both false positive and false negative. and is used to identify the best trust formation model as well as drop dead trust is the best application level threshold under which a node is considered misbehaving to optimize the application performance in false alarm probability.

Light Weight Intrusion Detection System is used to detect malicious nodes in the networks instead of intrusion detection system. The rest of the paper organized as follows. In Section II discuss about related work and contrast with existing work .In Section III is about Architecture model with process of SNs and CHs .In Section III discussed about modules .In Section IV is about Algorithms for Light weight intrusion detection system for activating monitor nodes and its global detection. Finally in Section V is about conclusion and future work.

II. RELATED WORK

Over the past few years, several protocols exploring the tradeoff Performance of energy consumption and QoS are used to maximize the system lifetime in HWSNs.In [2] ,Sensor nodes are divided into several groups whose total energies are same, it is not only extends the network lifetime but also applicable to the multilevel heterogeneous wireless sensor networks. In[4],Intrusion detection problem should be detected by intrusion detection system(IDS) to WSNs security infrastructure and it can detects unsafe activities and unauthorized login/access, when attacks occurred means it can notifies by different warnings and operates required actions. In[3],WSNs have limited power, more efficient energy is needed to maximize the network lifetime here multipath routing is used instead of single path routing because it uses the same optimal path again and again cause certain nodes to deplete their energy and cause network partition. Multipath routing is used to tackle network partition and decreasing message overhead and helps to improve the network lifetime.

Black hole is one of the most malicious attacks that target sensors routing protocols and to protect sensor network from black hole attacks by hierarchical energy efficient intrusion detection system [8].In [9], Green firewall used to protect WSNs against attacks in networks with less energy consumption and it isolate the intruder in WSns with less energy consumption. In [10], Security methods effectively detect attacks occur simultaneously in sensor networks here 4 types of keys: 1) A new individual key set 2) A pair wise key 3) A new cluster key and 4) A group key are used to enhance the energy consumption in sensor network and maintain detection power when an false data injection attack (FDIA) and false hello flood attack (FHFA) occur at same time.

Aggregation is a process ,which is applied to set of data, results in an output that is an improved representation of input and improvements are suggested in form of accuracy, completeness, relevance, reliability, energy conservation and efficiency and this technique used in distributed manner to improve lifetime and energy conservation of WSNs. In senor networks, input may comprise of data sensed by one sensor collected over a period also called temporal aggregation or form a no of sensors of same or different dimensionalities also called as spatial aggregation [11].Detection algorithms for WSNs detects collision attack based on the packet flow rate to base station node in the network. To protect WSNs and privacy of users collision attacks are used to consume the short power energy and it is difficult to detect it [12].

Trust management consists of heterogeneous sensor networks with different energy levels and different degrees of malicious(or) selfish behaviors in which SN adjust its behavior with clustered WSNs.CH consuming more energy than SNs on the other hand, selfish node consumes less energy than unselfish node and various attacks are performed by compromised SNs.Considering hierarchical trust management protocol is resilient to various attacks such as black hole attacks, slandering attacks, good mouthing attack recommending a bad node as a good node and bad mouthing attacks recommending a bad node as a good node in trust based routing applications[5].In [6],to measure level of trust among Intrusion detection systems (IDSes) in drichlet based trust management. Each IDSes to manage their trustworthiness base on acquaintances.

Trust based sensor nodes and data aggregators based on secure reliable data aggregation protocol called SELDA and sensor nodes exchange their trust levels with neighbor nodes to form a web of trust that allows them to determine secure and reliable paths to data aggregator(S) over one or more secure paths and data aggregator weight based on trust levels of sender nodes during data aggregation [7].

III. ARCHITECTURE MODEL

The Architecture model (fig A) represents the working process of SNs and CHs to achieve the QoS, Energy and Security. The SNs node is to be created in the network for each and every SNs nodes clusters are to formed based on clusters select CHs for each and every clusters here CHs are able to communicate with another CHs and to know the location of SNs and vice versa.CHs only gives Query to the SNs based on time if the node not gives the query on time means CHs knows that Query fails i, e node is also to be considered as a bad node. To avoid this problem and to remove the malicious node in the network voting distributed algorithm are used. Intruder can attack the system means energy should not be

efficient to achieve. The main aim is that to decrease the energy loss in networks and to increase the QoS.Trust systems are used to detect whether node is good node or bad node and pair wise key is used between both CHs and SNs to achieve high security.

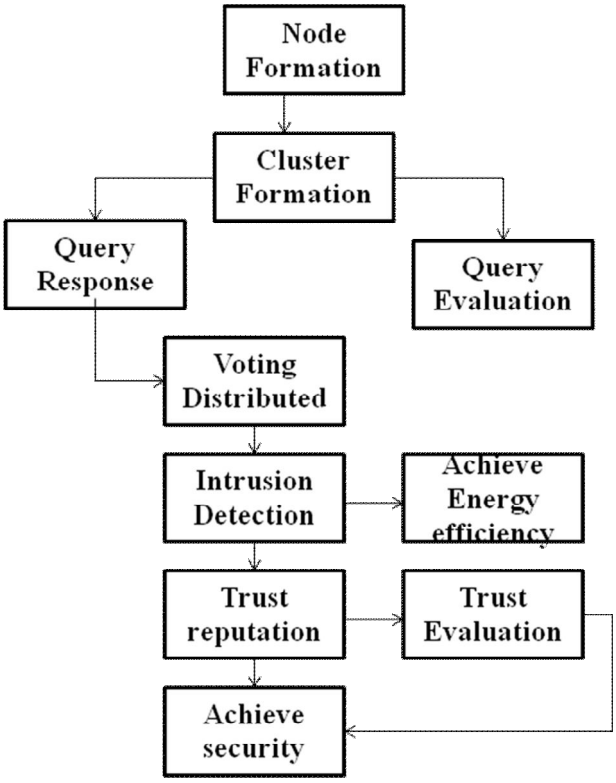

Figure: A. Architecture design

B. Network Formation

The dynamic network formation is based on node creation and node connection in WSNs. Node creation is based on set of node deployment and node deployment is based on number of nodes creation, here the source and destination are selected. Finally data transmission is occurred between the sources to destination based on hop by hop routing.

C .Cluster Formation

Energy optimized cluster formation for a set of randomly scattered wireless sensors is presented. Within a cluster of sensors are expected to be communicating with CH only. The cluster head summarize and process sensor data from the clusters and maintain the link with base station. Clustering is driven by minimization of energy for all the sensors.

D. Query Evaluation

Queries can be issued anywhere in HWSN by user ,through a nearby CH.A CH which takes a query to process is called query processing center(PC) and source redundancy by which m_s SNs sensing a

physical phenomenon in the same feature zone are used to forward sensing data to their CH node. Path redundancy by which m paths are used to relay packets from the source CH to the PC through intermediate CHs.

E. Distributed Voting Mechanism

Every CH also creates a pair wise key with every other CH thus a pair wise key exists for secure communication between nodes. To remove malicious nodes from the system a voting -based distributed IDS is applied periodically in every minute interval. A CH is being accessed its neighbor CHs, and a SN is being accessed by its neighbor SNs.In each interval, m neighbor nodes (at the CH or SN level) around a target node. Collecting the votes based on their host IDS results to collectively decide if the target node is still a good node.

F. Trust Evaluation

Trust enables a subset of the nodes to evaluate the behavior of neighboring nodes and make decision about them. Trust values are usually obtained taking into considerations different parameters such as personal reference also known as direct trust and also getting recommendations from the neighboring nodes i.e. reference also known as indirect trust and these parameters provided us a better assessment of trustworthiness.

G Assessment

Performance of algorithm is evaluated by using graph representation. It shows that proposed framework is able to adopt to changes in time parameters values while other approaches cannot. The performance gap between the proposed framework and other approaches is at the high level compare to other approaches .It provides better flexibility in the query processing center.

1V. ALGORITHMS FOR LIGHT WEIGHT INTRUSION DETECTION SYSTEM

The objective of Light weight intrusion detection System can easily be deployed in any node of a network, with minimal disruptions to operations. Easily be configured by system administrators who need to implement a specific security solution in a short amount of time. It is small, powerful and flexible enough to be used as permanent elements of the network security infrastructure.

In the Detection Algorithm no malicious nodes appear during the initial stage of sensor node deployment.SNs maintains two databases namely: 1) Malicious nodes and 2) Neighbor knowledge in the neighbor knowledge, broadcasting protocols are used to reduce the number of transmissions. And to detect the warm hole attacks in WSNs. In the malicious nodes, malicious counter have suspicious node stored in a CH crosses a threshold x means CHs creates and propagate a new rule to each and every SNs node in cluster. Then SNs update a new rule and add entry to its malicious database and malicious node is isolated from cluster and not involved in communication in the networks.

In algorithm 1, SNs receives a packet from a sensor in the network. If source node's ID is in its black list then the sender node uses local function () to drop the packet. Both source and destination nodes are one-hop neighbors; triggers the Global-detection function.


```
Communication Node
1.  Repeat <listen to the packet>
2.   Check<packet header>
3.    If{ID=destination node's ID}{
4.    If Local-Detection (packet)
5.      Then drop (packet)
6.    Else receive (packet);
7.       }
8.  And If (source & destination's ID,1
Hop neighbor)
9.          Then Global detection (packet)
10.   Else Drop (packet)
11. Until No transmission
```

Algorithm 1. Activating monitor nodes.

In algorithm 2, Global detection modules uses two – hop neighbor Knowledge and routing rules to detect anomalies within their transmission ranges.

```
Global-detection (packet)
1. {
2.  If Looking (packet_i _id, buffer)
3.  Then {
4.   If Check (node's ID, 2 hop neighbor's
5.      List)
6.    Or Check (packet_i, predefined-rules)
7.  Then {
8.        Create (alert);
9.        Send (alert, cluster-head);
10      }
11.  }
```

Algorithm 2. Global detection at monitor nodes.

V. CONCLUSION AND FUTURE WORK

This paper describes to decrease energy loss and to increase QoS and high security by using pair wise key is used. lifetime of heterogeneous wireless sensor networks is also maximized while satisfying the reliability, timeliness and security requirements in the presence of unreliable wireless communication and malicious nodes .and Trust/reputation management system is also used to strengthen intrusion detection through "Weighted Voting" mechanisms and Finally Light Weight Intrusion Detection System algorithm is the efficient way to detect malicious nodes in networks. For Future Work, the more efficient

trust based system are used, where concurrent query traffic is heavy means trust based admission control is used and to optimize application performance.

REFERENCES

[1] Hamid Al-Hamadi and Ing-Ray Chen, "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks" IEEE Trans. Networking., vol.10, 2013

[2] jiun-jian liaw,lin-huang chang and hung-chi chu, Improving Lifetime in Heterogeneous Wireless Sensor Networks with The Energy-Efficient Grouping Protocol "In "l J.Inno.Comput.inf. and Ctrl., vol 8,no.9 ,2012.

[3] Kewei Sha,Jegnesh Gehlot and Robert Greve "Multipath Routing Techniques in Wireless Sensor Networks".

[4] Hoseein Jadidoleslamy,"A hierarchical Intrusion Detection Architecture for Wireless Sensor Networks IJNSA, vol.3, no.5, 2011.

[5] F. Bao, I. R. Chen, M. Chang, and J. Cho, "Hierarchical trust Management for Wireless Sensor Networks and its Application to
Trust Based Routing and Intrusion Detection",IEEE Trans. Netw. Service Manag., vol.9, no.2,pp ,161-183,2012.

[6] C.j Fung,z. jie I.Aib and R. Boutaba. "Drichlet-based Trust Management for Effective Collaborative Intrusion Detection networks", IEEE Trans.Netw.Service Manag., vol.8,no.2,pp.79-91,2011

[7] S. Ozdemir," Secure and reliable data aggregation for Wireless Sensor networks", Proceedings of the 4th international conference on ubiquitous computing systems, Tokyo, japan, 2007.

[8] Enrique J.Duarate-Melo, Mingyan Liu EECS, University of Michigan,Ann Arbor " Analysis of Heterogeneous Wireless Sensor Networks".

[9] Ping Yi,ting Zhu,Qingquan Zhang,Yue Wu,Jianhua Li "School Of Information Security Engineering, China " Green Firewall: An energy-efficient Intrusion Prevention Mechanism in Wireless Sensor Networks".

[10] Su Man Nam and Tae Ho Cho, "An Energy Efficient Countermeasure against multiple attacks of the false data injection attack and false hello flood attack in the Sensor Networks.

[11] Qurat ul-Ain I.Tarriq, Saneeha Ahmed, Huma Zia "An Objective based Classification of Aggregation Techniques For Wireless Sensor Networks.

[12] Hosamsoleman, Ali Payandeh,Nasser Mozayyani, Saeedsedighiankashi "Detection Collision Attacks in Wireless Sensor Networks usingrule-based Packet Flow rate", IJERA vol 3,issue 4,2013.

Authors Bibliography

MS.B.Divya has received the B.Tech (IT) from Chettinad College of Engineering in 2012 and Pursuing M.Tech (IT) in V.S.B Engineering College, Anna University Chennai .Areas of interest includes Networking, Cloud Computing, WSNs.

MS.R.Manju received the BE (Computer Science and Engineering) from Sakthi Mariamman Engineering College in 2011 and pursuing M.Tech (Information Technology) in VSB Engineering College, Anna University, Chennai. Areas of interest include Data Mining and Cloud Computing.

MS.B.Sathyabama received the B.Tech (Information Technology) from Kalasalingam University in 2012 and Pursuing M.Tech (Information Technology) in VSB Engineering College, Anna University, Chennai. Area of Interest includes Data Mining and Networks.

