Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

WATCHDOG OPTIMIZATION TECHNIQUE IN WIRELESS NETWORK

Praveen Kumar, M.Tech (Computer)

Department of Computer Engineering, Bharti Vidyapeeth (to be Deemed University), pune
Guide Name: - Prof S.D Joshi (Dean, Faculty of Engineering and Technology, Pune)

ABSTRACT

1. INTRODUCTION

A wireless sensor network is an ad-hoc network which consists of large number of small inexpensive devices which are known as nodes (motes). These nodes are battery operated devices capable of communicating with each other without relying on any fixed infrastructure. The wireless sensor networks (WSNs) are often deployed in such an environment which is physically insecure and we can hardly prevent attackers from the physical access to these devices. WSN consists of base station along with number of nodes that sense the environment and send data to the base station. The base station (sink) is more powerful than other nodes in terms of energy consumption and other parameters and serves as an interface to the outer world. When any node needs to send a message to the base station that is outside of its radio range, it sends it through internal nodes. The internal nodes deployed in WSNs are the same as others, but besides of local sensing they also provide forwarding service for other nodes. A Wireless Sensor Network (WSN) is a specialized wireless network that is composed of a number of sensor nodes deployed in a specified area for monitoring environment conditions such as temperature, air pressure, humidity, light, motion or vibration, and can communicate with each other using a wireless radio device. WSNs are powerful in that they are amenable to support a lot of very different real-world applications; they are also a challenging research and engineering problem because of this very flexibility. Most sensor network protocols assume a high degree of trust between nodes in order to eliminate the overhead of authentication. A watchdog system is a method of behavioral monitoring of sensor nodes. In such a system, a number of sensor nodes are selected as watchdogs. It is considered as an effective countermeasure to various attacks such as denial-of-service (DoS), sinkhole, and selective forwarding. Watchdogs are deployed to detect misbehaving nodes in a WSN. Each watchdog is responsible for its single hop neighbors. It may overhear neighbors promiscuously or communicate with them for behavioral monitoring. It periodically sends behavioral reports to the base station (BS). It is also responsible for event driven reporting when anomalies are detected. As watchdogs are mainly dedicated to the monitorial tasks, sensing operations lose resources. Optimal selection of watchdogs can reduce resource consumptions in monitorial tasks.

2. LITERATURE SURVEY

Table 1. Survey Table

Sr. No.	Paper Name	Author Name	Published Year	Advantages	Disadvantages
1	A Survey of Intrusion Detection Systems in Wireless Sensor Networks [1]	Ismail Butun, Salvatore D. Morgera, and Ravi Sankar	2014	Intrusions detected before attackers can harm the network	Only used in MANET network.
2	When WatchDog Meets Coding [2]	Guanfeng Liang and Nitin Vaidya	2010	Attacker will be detected with high probability while achieving throughput arbitrarily close to optimal	Watchdog can only observe a fraction of packets.
3	Toward Energy-	Peng Zhou, Siwei	2015	Minimize the	Less efficiency.

	Efficient Trust System Through Watchdog Optimization for WSNs [3]	Jiang		energy cost of watchdog usage.	
4	On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks [4]	Abror Abduvaliyev, Al-Sakib Khan Pathan	2013	Effectively detect IDS system.	Only applicable for WSN.

In [1] authors proposed an Intrusion Detection Systems (IDSs) that are proposed for WSNs is presented. Firstly, detailed information about IDSs is provided. Secondly, a brief survey of IDSs proposed forMobile Ad-Hoc Networks (MANETs) is presented and applicability of those systems to WSNs is discussed. Thirdly, IDSs proposed for WSNs are presented.

In [2] authors first show that even if a watchdog can overhear all packet transmissions of a flow, any linear operation of the overheard packets can not eliminate missdetection and is inefficient in terms of bandwidth. Alos propose a lightweigh misbehavior detection scheme which integrates the idea of watchdogs and error detection coding.

In [3] authors disclose the ineffective use of watchdog system in existing trust system, and thereby propose a suite of optimization methods to minimize the energy cost of watchdog usage, while keeping the system's security in a sufficient level.

In [4] authors worked on Intrusion Detection Systems (IDS) in WSNs, and presents a comprehensive classification of various IDS to detect anomaly detection, misuse detection, and specification-based detection Protocols.

3. EXISTING SYSTEM

The statistical decision-making framework approach extends our earlier work in where a heuristic probabilistic routing algorithm was proposed to enhance the privacy for the destination node. It always compromise user's privacy. Three common approaches to mitigate analysis attempts are to: (i) change the physical appearance of each packet at every hop via hop-by-hop encryptions (ii) introduce transmission delays at each hop to de-correlate traffic flows, or (iii) introduce dummy traffic to obfuscate traffic patterns. The first two approaches may not be desirable for low-cost or battery-powered wireless networks, e.g., wireless sensor networks as (i) the low-cost nodes may not be able to afford using the computationally expensive encryptions at each hop, and (ii) introducing delays at the intermediate nodes may not be effective when there is little traffic in the network. Therefore, we use the dummy traffic approach to provide privacy by lowering the adversary's detection rates in a wireless network. Specifically, we consider an adversary that uses the optimal maximum-a-posteriori (MAP) estimation strategy.

3.1. Disadvantages of Existing System

1. There is no guarantee of the transmission cost; latency will be done properly in network.
2. Delays at the intermediate nodes may not be effective when there is little traffic in the network.
3. Nodes may not be able to afford using the computationally expensive encryptions at each hop.

4. PROPOSED SYSTEM

A Wireless Sensor Network (WSN) is a specialized wireless network that is composed of a numerous of sensor nodes deployed in a specified region for monitoring environment conditions such this kind of as temperature, air pressure, humidity, light, motion or vibration, and can communicate with each and every other making use of a wireless radio device. WSNs are effective in that they are amenable to support a lot of extremely different real-world applications; they are also a difficult research and engineering issue simply because of this extremely flexibility. Most sensor network protocols assume a higher degree of trust in between nodes in order to eliminate the overhead of authentication. A watchdog system is a method of behavioral monitoring of sensor nodes. In this kind of a system, a numerous of sensor nodes are selected as watchdogs. It is considered as an effective countermeasure to different attacks such as denial-of-service (DoS), sinkhole, and selective forwarding. Watchdogs are deployed to detect misbehaving nodes in a WSN. Each and every watchdog is responsible for its single hop neighbors. It may possibly overhear neighbors promiscuously or communicate with them for behavioral monitoring. It periodically sends behavioral reports to the base station (BS). It is also responsible for event driven reporting

when anomalies are detected. As watchdogs are mostly focused to the monitorial tasks, sensing operations lose resources. Optimal selection of watchdogs can decrease resource consumptions in monitorial tasks. The presented models provide a much better understanding resource effective watchdog deployment approaches. This system presents KNN algorithm to optimize the watchdog selection for nodes. It will also detect the malicious activity of node in network.

4.1 Advantages of Proposed System

1. It cannot compromises users privacy.
2. It provides proper the transmission in network.
3. Optimize the watchdog selection for nodes.

5. SYSTEM ARCHITECTURE

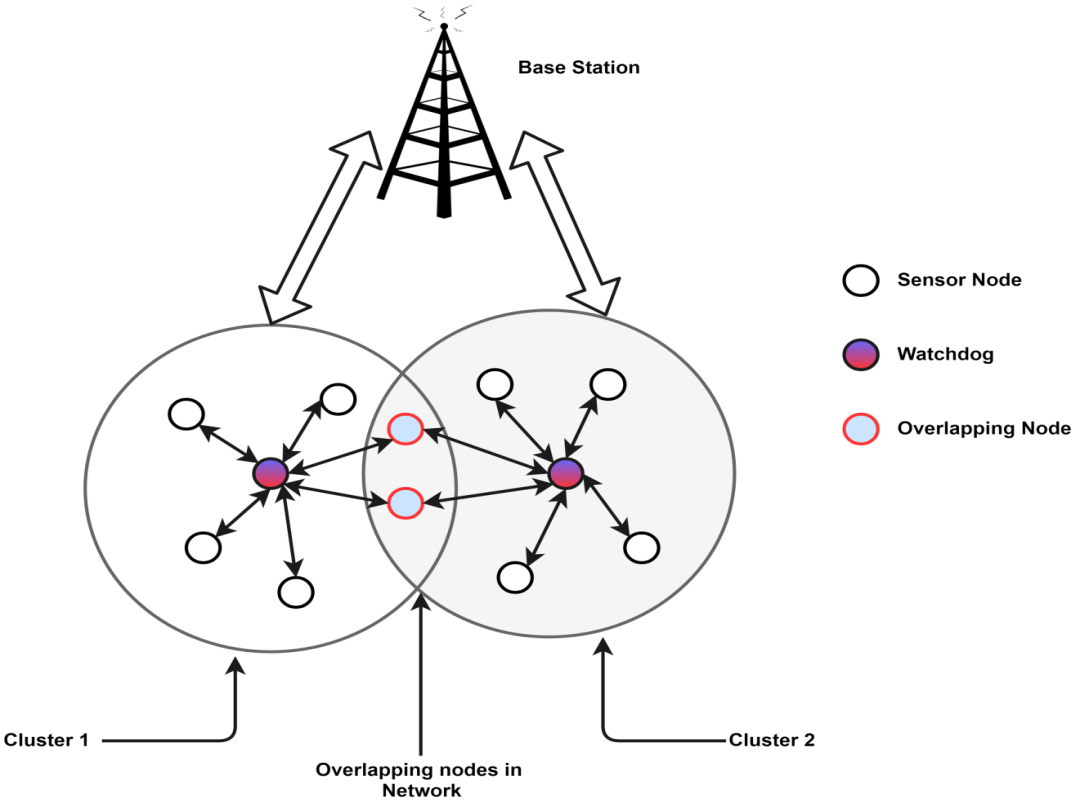

Figure 1. Architecture of Proposed System

There are two clusters on two different pcs each cluster is having cluster head who is having highest weight among all the nodes in the cluster. The weight will be calculated as per the kernel battery of pcs. Creating a two cluster as per the battery status like 10%-30% and 30%-100%. Here we have to get the overlapping node in cluster. In this CH can see the entire cluster nodes, there data, and status. Status column shows the whether particular node has been malicious or not.

a. Send data:

In this the CH head will send data to another CH if node wants to communicate with another CH.

b. Receive date:

In this the CH will receive the data between nodes or also from other CH nodes.

Assume there are one cluster with 8 nodes on pc1 which is having the battery of 10-%30% and other second cluster with 8 nodes on pc2 having battery of 30%-100%.

Scenario 1:

In this if the first cluster is having 8 nodes and second cluster is also having 8 nodes on network. Nodes are having the same battery backup in both the clusters.

For example, if one cluster contains the nodes in network which is having the battery backup of 10%-30% and second cluster is also having the battery backup of 30%-100%. At this time the nodes which are having the battery of 25% but these nodes are also consumes the energy of both the cluster. At this time the Watchdog system will remove the overlapping nodes in network by applying KNN algorithm for classifying the nodes into a particular cluster. So it can remove the overlapping nodes into network.

Scenario 2:

Any node which is having highest kernel battery backup it will be declared as a Cluster head (CH) of that particular cluster.

Scenario 3:

For example, if CH1 nodes wants to communicate with other CH2 nodes or send the data. Then first nodes have to request the particular CH that he wants to send the data to CH2 node. Then CH1 request to CH2 that accept the request and receive data.

c. Base Station:

View the malicious node report which is send by the watch dog.

6. ALGORITHM:

A. Blowfish

Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time. This algorithm is divided into two parts.

1. Key-expansion
2. Data Encryption

1.1 Key-expansion:

It will convert a key of at most 448 bits into several sub key arrays totaling 4168 bytes. Blowfish uses large number of sub keys.

These keys are generate earlier to any data encryption or decryption.

The p-array consists of 18, 32-bit subkeys:

P1,P2,……..,P18

Four 32-bit S-Boxes consists of 256 entries each:

S1,0, S1,1,……. S1,255

S2,0, S2,1,…….. S2,255

S3,0, S3,1,…….. S3,255

S4,0, S4,1,.....S4,255

Generating the Subkeys:

The subkeys are calculated using the Blowfish algorithm:

1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.
2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)
3. Encrypt the all-zero string with the Blowfish algorithm, using the subkeys described in steps (1) and (2).
4. Replace P1 and P2 with the output of step (3).

5. Encrypt the output of step (3) using the Blowfish algorithm with the modified subkeys.
6. Replace P3 and P4 with the output of step (5).
7. Continue the process, replacing all entries of the P array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm.

In total, 521 iterations are required to generate all required subkeys. Applications can store the subkeys rather than execute this derivation process multiple times.

1.2 Data Encryption:

It is having a function to iterate 16 times of network. Each round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round.

B. KNN:

C. Determine parameter k = number of nearest neighbor.
D. Calculate the distance between the query instance and all the training samples.
E. Sort the distance and determine nearest neighbor based on th k th minimum distance.
F. Gather the category y of the nearest neighbor.
G. Use simple majority of the category of nearest neighbor as the prediction value of query instance.

7. CONCLUSION

We designed Watchdog system which is a monitoring technique and which detects the misbehaving nodes in the network. Watchdog technique is a fundamental building block to many trust systems that are designed for securing wireless sensor networks (WSNs). Optimizing the watchdog techniques can save energy without sacrificing much and also enhance the protection against certain attacks. To optimize this we have used the KNN algorithm.

REFERENCES

[1] Butun, Ismail, Salvatore D. Morgera, and Ravi Sankar. "A survey of intrusion detection systems in wireless sensor networks." IEEE communications surveys & tutorials 16.1 (2014): 266-282.
[2] Liang, Guanfeng, Rachit Agarwal, and Nitin Vaidya. "When watchdog meets coding." INFOCOM, 2010 Proceedings IEEE. IEEE, 2010.
[3] Zhou, Peng, et al. "Toward energy-efficient trust system through watchdog optimization for WSNs." IEEE Transactions on Information Forensics and Security 10.3 (2015): 613-625.
[4] Abduvaliyev, Abror, et al. "On the vital areas of intrusion detection systems in wireless sensor networks." IEEE Communications Surveys & Tutorials 15.3 (2013): 1223-1237.

