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. 4, Issue. 5, May 2015, pg.591 – 597

RESEARCH ARTICLE

An Efficient Way to Evaluate Statistical Source Anonymity in Wireless Sensor Network

Harshal S. Bhagwat[1], Prof. Poonam P. Borkar[2]

[1]Computer Science and Engineering Department & S.G.B.A. University, India

[2]Computer Science and Engineering Department & S.G.B.A. University, India

[1] harshalbhagwat123@gmail.com; [2] poonam.borkar@raisoni.net

Abstract* — *Wireless sensor network is another different network in which communication will be done with the sensors node. In WSN, some applications, the locations of events remain anonymous reported by a sensor network. That is, only authorized observers or person be able to communicate with each other. The novelty of the proposed approach introduce the notion of "interval indistinguishability". We are here propose a key pre-distribution scheme for wireless sensor network which provides a good secure connectivity to all nodes which are in coverage. This key approach is a very important concept for many security services such as authentication and confidentiality which are required to provide secure communication in WSN. For deploying this above two scenario, conduct simulations regarding different constrained including data delivery ratio, end-to-end delay ratio. The obtained results show that, this approach achieves source anonymity bound which is better than previous literature security for WSN, and output will be shown with graph of end-to-end delay and data delivery ratio.

Keywords*— *Indistinguishability, End-to-end, Simulations, WSN (Wireless Sensor Network)

I. INTRODUCTION

Wireless sensor network are having spatially distributed autonomous sensors to monitor or for watching physical such as vehicle health monitoring system, human body temperature or environmental conditions, such as temperature, sound, pressure, agriculture activities etc. and to cooperatively passing to the base station. The advance development of wireless sensor networks for security purposes was motivated by military applications such as battlefield and surveillance; now a days such sensor networks are used not only in many industrial but also in consumer applications, like monitoring and control, machine health monitoring system. The main reason behind is that in military applications, there are high risk of transmitting information. So that, it is necessary to transmit that information in a very careful manner. The WSN is built from small nodes and structure is same as one computer connected with another node in a laboratory. A sensor node might vary in size from that of a compass box to the size of a grain of stone, and many small sensors have yet to be created. The sensor node cost is similarly change, its ranging from a few to hundreds to thousand rupees depending on the functionalities of the sensor nodes.

WSNs are highly resource constrained. Implementation of source anonymity in wireless sensor network is achievable but to secure that network coverage any solution is there? This question motivates to implement key distribution approach that provide solution on above problem. Therefore, it is essential to design smart techniques to build blocks of keys that will be embedded on the nodes to secure the network links. This motivates the use of pre-distributed key approach that allows a smart building of blocks with unique features that allow to cope with the connectivity issues.

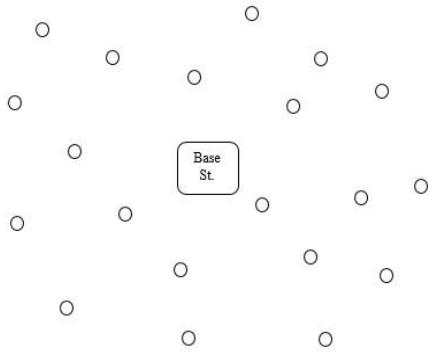

Figure 1: A generic view of wireless sensor network

Figure 1 shows a generic view of wireless sensor network having sensor nodes shown by small circle and base station which will show by small box.

II. LITERATURE SURVEY

In [1] & [2] B. Alomair et al. introduces a framework based on binary hypothesis testing for statistical source anonymity in wireless sensor networks for modelling, analysing, and evaluation. Also introduced the approach of interval in distinguishability to model source location privacy. Showed that the previous approaches for design anonymous systems introduce real intervals while fake intervals are uncorrelated in wireless sensor network. The problem of catching source information means real and fake data to the statistical problem of binary hypothesis testing, and studied why previous approaches are unable to detect the source of information dropped that was demonstrated.

In [3] Ian F. Akyildiz et al. states that, in wireless communications and electronics recent advancement has given the development in wireless sensor networks has low cost nodes. In various application areas, the sensor networks are used for such as health, military, home, irrigation, forest, landslides and etc. For different application areas, there are various technological issues that researchers are currently resolving. In this wireless sensor networks is captured in this literature, where solutions to the problems are discussed under their related protocol. This article points out the research technical issues and motivates to new interests and developments in this wireless sensor network field.

In [4] Jennifer Yick et al. surveyed on three different issues as, internal platform and underlying operating system, communication protocol stack, and network services, provisioning, and deployment issues. Here compared different proposed designs, algorithms, protocols, and services. Moreover, here highlighted possible improvements and research area. There are still many issues to be resolved around WSN applications such as communication architectures, security and management. And by solving these issues, can close the gap between technology and application.

In [5] Mauro Conti et al. provided a survey of the literature in source location privacy (SLP) for wireless sensor networks (WSNs). Then, discussed some of the works that have a high influence on the state of the art today, together with the concepts that they introduced. These concepts included anonymity, observability, safety period, capture likelihood, unsinkability, contextual privacy, identity privacy, location privacy, timing privacy, and route privacy. Next, included a classification of the adversary based on its behaviour, view of the network, and the information exposed by the network to the adversary.

In [6] Parv Venkitasubramaniam et al. provides the main contribution is an analytical approach to anonymous wireless networking. To the best of our knowledge, the proposed metric is the first analytical measure designed to quantify the secrecy of routes in an eavesdropped wireless network. The preliminary results obtained so far clearly demonstrate the potential for analytical methods to address the scheduling design. Furthermore, results also present connections to classical information theoretic problems such as wire tapped channel communication and rate distortion, now present novel applications.

In [7] Walid Bechkit et al. proposed work for a scalable key management scheme in WSNs. And make use, for the first time, of the unital design theory. Showed that a basic overlapping from unital to key pre-distribution allow to get an extremely high network resiliency while giving a low direct secure connectivity coverage. And

proposed then an efficient scalable unital-based pre-distribution scheme for key providing high network also good secure connectivity coverage. In this literature, conducted analytical analysis and simulations to compare new solution to existing ones, the results showed that this approach provides a good secure network coverage of large scale networks with a low key storage and a good network scalability.

III. OBJECTIVES

To design an efficient source anonymity for WSNs that provide secularism to source node which transmitted the sensed events in the network. Here to secure sensed events at source node, we design such a system that not only provide source anonymity but also provide secure network coverage i.e. WSN. And here we analyse AODV protocol for WSNs that guarantees in delivering messages with a packet delivery ratio, and on the other hand with end-to-end delay.

IV. PROPOSED WORK

In this proposed work, there are two approaches have been executed, first one is statistical source anonymity approach, and second one is key pre-distribution scenario for WSN.

4.1 Approach for Statistical Source Anonymity

In this section, introduce the source anonymity model for wireless sensor networks. The main working of SSA is interval indistinguishability.

4.1.1 Interval Indistinguishability

Currently, statistical source anonymity in wireless sensor networks is created by the adversary's capability to distinguish or to get statistical analysis between real and fake transmissions. In this given series of transmissions of a certain node means real and fake messages, the adversary cannot able to distinguish, with significant confidence or get that information, which transmission from source node carries real information and which transmission from source node is fake, only the number of transmissions the adversary can observe. Here also consider now an adversary monitoring a wireless sensor network over various time intervals. And assume that, the adversary during a given time interval, is able to get a change in the statistical behaviours in the network of transmission times of a certain node which will be transmitted from source node to destination.

4.2 Approach for Pre-Distribution of Key

In this section, present a new key pre-distribution scheme for WSNs. In order to enhance the key sharing probability while maintaining high secure network, propose to build the blocks and preload each node with a number of keys picked in a selective way.

4.2.1 Random Key Pre-Distribution

Main goal of a key management scheme is to ensure confidentiality of information. Also, keys can be helpful in authenticating legitimate nodes. An adversary may try to crack secret key and extract confidential information from the messages exchanged between communicating nodes. If keys are used for authentication purposes, adversary may try to act as a legitimate node and try to extract confidential information from other nodes. While trying to crack a secret key, adversaries try to learn message patterns and guess the secret key. Also, they try to save some encrypted messages, which they can replay later on. In order to prevent adversaries from guessing secret keys, it is important to refresh keys at appropriate time intervals. Time intervals depend upon frequency of communication and frequency of key usage. Apart from trying to crack secret information, adversary can also harm a sensor network in several other ways. It can try to jam wireless signals of a sensor networks. Also, it can try to create noises and disrupt communication. In other words, adversary can carry out denial-of-service attacks. Apart from that, an adversary can try to drain sensor nodes' energy by initiating bogus messages or replaying old messages.

In wireless sensor networks, it is not necessary that keys are established among every pair of sensor nodes. For a wireless sensor network to work, it is important that every sensor node gets sufficient bandwidth and neighbouring nodes, who can relay its messages to the base station through various paths. For example, if node A has 15 nodes in its neighbourhoods, it can establish pair-wise keys with only 4 of them and those 4 neighbouring nodes can provide node A distinct routes to the base station, then node A does not need to establish pair-wise keys with rest of the 11 node. In the first phase of their scheme, a key ring of K keys and their identifiers is stored in the memory of each node prior to deployment. Every pair of nodes shares a key with some probability. In discovery phase, every node broadcasts its key identifiers and challenges to find those nodes, with which it shares a key. If some keys are left unused after the discovery phase, they can be used to

establish keys between nodes, who do not share a common key. For example, node A shares a key x with node B and node B shares another key y with node C while nodes A and C do not share a key. If node B has a key z, which it does not share with any node, it can send key z to both node A and node C so that they can communication with each other using z. In this scheme, there are group keys that are shared between the base station and all other nodes. In order to revoke a compromised sensor node, the base station compiles the list of keys known to the compromised node, uses a group key to sign the list and broadcasts it into the network using another one. Upon receiving the list, all nodes delete the keys, which are known to the compromised node, from their memory.

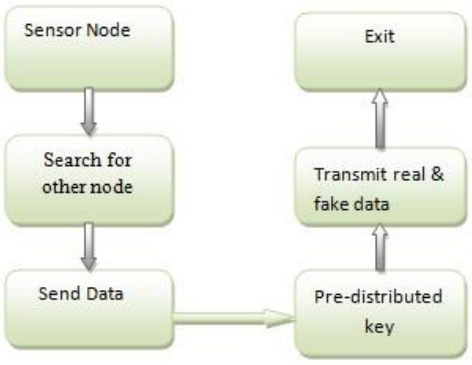

Figure 2: Proposed system diagram

V. EXPERIMENTAL RESULTS

In this, experimental results are drawn with the help of Network Simulator 2 (NS2) tool in graph scenario. And here we analyse routing protocols for WSNs that guarantees in delivering messages with a packet delivery ratio, and on the other hand with end-to-end delay.

5.1 Performance Metrics

5.1.1 Source Anonymity Bound

Source anonymity can be defined as, real message probabilistic to fake message probabilistic ratio.

$$SA = \frac{PR}{PF}$$

Here in above equation, SA denote for source anonymity bound, PR denote the real message probabilistic and PF shows the fake messages probabilistic.

For source anonymity metrics, we are taken 20 trials for different source node and we get results as below,

Table 1: Anonymity bound

PR>PF	PR<PF	PR=PF	Anonymity bound
8	12	0	0.745

PR >PF denotes larger correlation coefficient in real intervals, PR <PF denotes larger correlation coefficient in fake intervals, while PR=PF denotes equal correlation coefficient in real and fake intervals. The simulation results are obtained from 20 independent trials. In previous results anonymity bound is as 0.539 and our results shows 0.745. Hence obtained results are better than the previous system.

5.1.1 Packet Delivery Ratio

Packet delivery ratio can be defined as the ratio of the data packets delivered to the destinations to those generated by the sources. Sometimes it is known as Packet Delivery Fraction (PDF).It can defined as:

$$P = \frac{1}{C}\sum_{f=1}^{c}\frac{Rf}{Nf}$$

Where P is the fraction of successfully delivered packets, C is the total number of flow or connections, f is the unique flow id serving as index, Rf is the count of packets received from flow f and Nf is the count of packets transmitted to f.

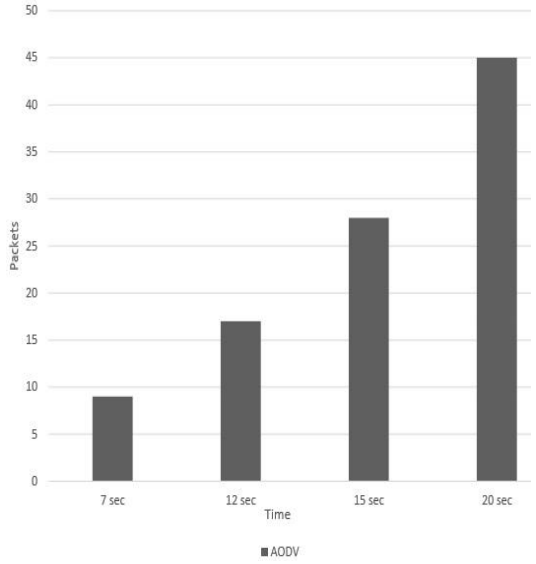

Fig 2: Data/Packet delivery ratio for real messages

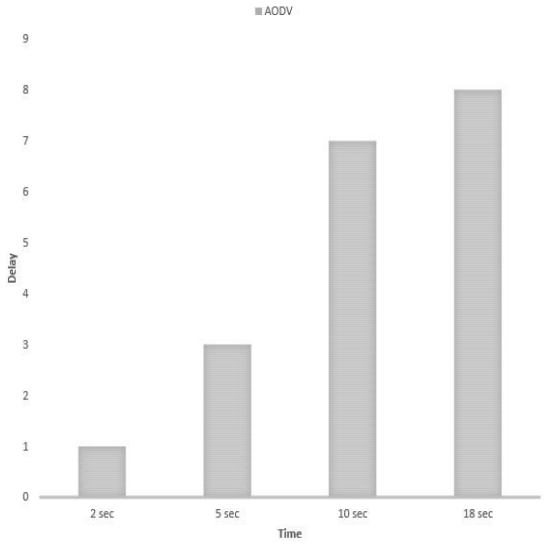

Fig 3: Data/Packet delivery ratio for fake messages

In this, graph will be drawn by the simulation tool. And this graph shows in time vs. packets form for delivered real and fake messages.

5.1.2 End-to-end Delay Ratio / Latency

It can be defined as the average time between packets sent and received. It can be defined as:

$$D = \frac{1}{N}\sum_{i=1}^{s}(ri - si)$$

Where N is the number of successfully received packets, i is unique packet identifier, ri is time at which a packet with unique id i is received, si is time at which a packet with unique id i is sent and D is measured in ms.

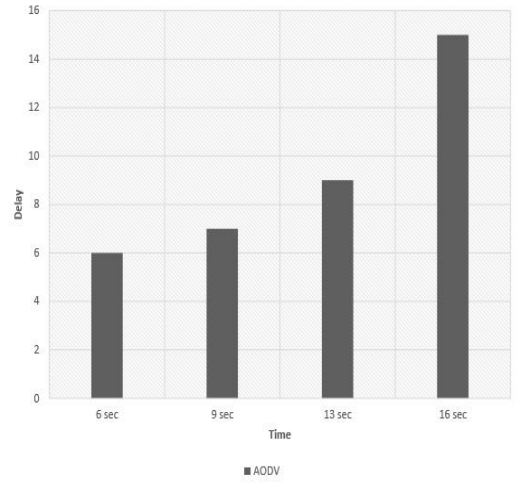

Fig 4: End-to-end delay ratio for real messages

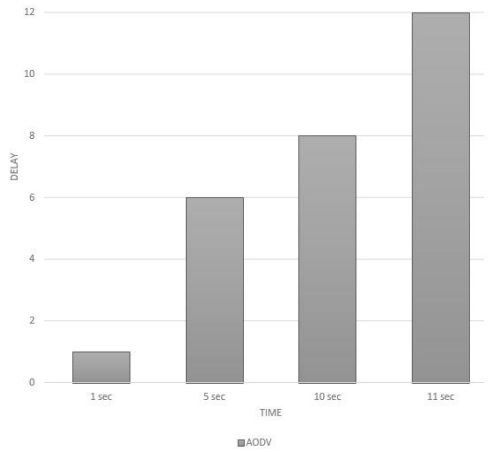

Fig 5: End-to-end delay ratio for fake messages

This chart shows end-to-end delivery ratio for real and fake messages. While transmitting real and fake messages form source to destination or we can say that to sink, it will be stored in trace file, and here shown into the chart form.

VI. CONCLUSIONS

Source location information privacy protection is a significant security property of sensor networks used to collect information about monitored events or objects in military monitoring applications. To this aim, SSA is proposed to provide strong protection for source location information privacy in WSNs. By using this SSA system, transmitting of sensed events in wireless sensor network in the presence of adversary is safe or in other words it is confidential. We can get solution on our source anonymity problem. That means the source location information (sensed data) is secure. Here we analyse routing protocol which are used in this approach. Using pre-distribution key scheme also provides a good secure connectivity coverage.

In this, key management is a very critical concern for many security objectives such as authentication and confidentiality & which are required to secure communication in WSN. This system also provide total secure connectivity coverage between nodes which are deployed in WSN & ensures good network resiliency. The obtained results show that, this approach achieves source anonymity or we can say that security for WSN, and output will be shown with graph for the constraints end-to-end delay and data delivery ratio. With the source anonymity bound results also shows that, our approach is better than previous approach.

REFERENCES

[1] Basel Alomair, Andrew Clark, Jorge Cuellar, and Radha Poovendran, "Toward a Statistical Framework for Source Anonymity in Sensor Networks", IEEE Transactions on Mobile Computing, Vol. 12, No. 2, February 2013.

[2] Basel Alomair, Andrew Clark, Jorge Cuellar, and Radha Poovendran, "Statistical Framework for Source Anonymity in Sensor Networks", IEEE GlobCom, 2010.

[3] Ian Akilydiz, Weilian Su, Yogesh Sankarasubramaniam, Erdal Cayirci, "Wireless Sensor Network: A Survey" Computer Networks, vol 38, no. 4, 2002.

[4] Jennifer Yick, Biswanath Mukherjee, Dipak Ghoshal, " Wireless Sensor network survey" Vol. 52, No. 12, Computer Networks, 2008.

[5] Mauro Conti, Jeroen Willemsen, and Bruno Crispo, "Providing Source Location Privacy in Wireless Sensor Networks: A Survey" IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, Third Quarter 2013.

[6] Parv Venkitasubramaniam, Ting He, Lang Tong, and Stephen B. Wicker, "Toward an Analytical Approach to Anonymous Wireless Networking" Security in Mobile Ad Hoc and Sensor Networks, February 2008.

[7] Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah and Vahid Tarokh, "A Highly Scalable Key Pre-distribution Scheme for Wireless Sensor Networks" IEEE Transactions on Wireless Communications Vol. 12 No. 2, 2013.

[8] Syed Raazi, Zeeshan pervez, Lee, "Key management schemes of wireless sensor networks: A survey".

[9] Julia Rahman, Md. Al Mehedi Hasan, Md. Khaled Ben Islam, "Comparative analysis the performance of AODV, DSDV and DSR Routing protocols in Wireless Sensor Network" International Conf. on ECE, December 2012.

[10] Cedric Ramassamy, Hacene Fouchal, Philippe Hunel, "Classification of Usual protocols over Wireless Sensor Networks" IEEE ICC 2012.

[11]Yun Li, Jian Ren, and Jie Wu, "Quantitative Measurement and Design of Source-Location Privacy Schemes for Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 7, July 2012.

[12] R. Velayutham, J. Mary Suganya, "Security Authentication through AES and Fine- Grained Distributed Data Access Conyrol Using Clustering in Wireless Sensor Networks," ICCCNT, July 2012.

[13] Julia Rahman, Md. Al Mehedi Hasan, Md. Khaled ben Islam, "Comparative Analysis the Performance of AODV, DSDV, and DSR Routing Protocols in Wireless Sensor Network," IEEE International Conference on Electrical and Computer Engineering, December 2012.

[14] Cedric Ramassamy Lamia, Hacene Foucjhal, Crestic, Philippe Hunel, "Classification of Usual Protocols over Wireless Sensor Networks," IEEE ICC Ad-hoc and Sensor Networking Symposium, 2012.

