Source Anonymity in WSNs using Real/Fake packet Injections

Anas Bushnag, Abdulshakour Abuzneid, Poster Advisor: Ausif Mahmood
Department of Engineering
University of Bridgeport, Bridgeport, CT

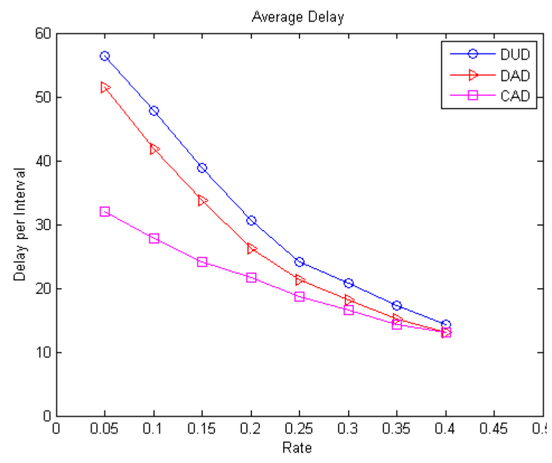
Abstract

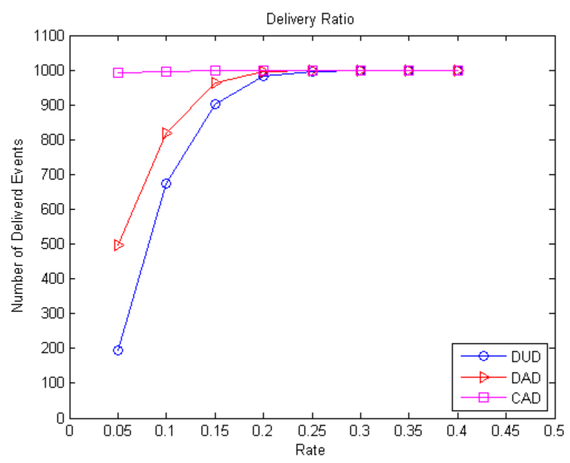
Many of Wireless Sensor Networks (*WSNs*) applications such as tracking and monitoring endangered species, and/or military applications in areas of interest require anonymity of the origin known as Source Location Privacy (*SLP*). The aim is to prevent unauthorized observers from tracing the source of a real event by analyzing the traffic on the network. Three different techniques: Dummy Uniform Distribution (*DUD*), Dummy Adaptive Distribution (*DAD*) and Controlled Dummy Adaptive Distribution (*CAD*) are introduced to overcome the anonymity problem against a global adversary (which has the capability of analyzing and monitoring the entire network). Our proposed techniques confuse the adversary about the existence of the real event by introducing low rate fake messages, which subsequently lead to location and time privacy. Simulation results demonstrate that the proposed techniques improve delivery ratio and reduce the delay and overhead of a real event's packets while keeping a high level of anonymity.

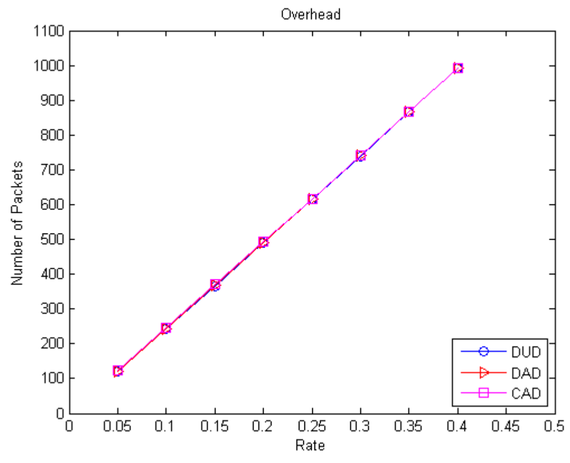
Proposed Techniques

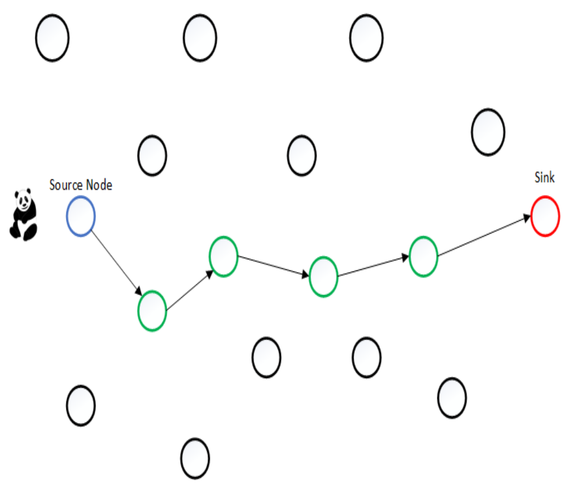
Injecting a dummy packet every interval for each node during the lifetime of the network consumes a huge amount of power and resources. So, the notion behind *DUD* is to have the same transmitting constant rate for both real and fake traffic. By applying this technique the adversary cannot recognize if the transmitted packet is real or dummy. In order to increase the delivery ratio of delivered real packets to total real packets, *DAD* is introduced and it works as follows. All nodes in the network will be categorized into dummy nodes and real nodes. At the beginning, all nodes will be considered as dummy nodes using a transmitting constant rate as *DUD*. However, if a node detects an event or forwards packets of a real event, it becomes a real node. A real node will increase the rate of its real traffic. Moreover, it decreases the rate of its fake traffic. Since *DUD* and *DAD* schemes could fail providing maximum delivery ratio. *CAD* is introduced to maximize the delivery ratio and minimize the delay to guarantee the arrival of all packets in the real event to the sink within the required window by the application. if a real node failed to transmit a real packet using the real traffic rate for n-intervals, this node will transmit the first real packet in its buffer without using any kind of probability (transmitting rate is one).

Simulations and Results

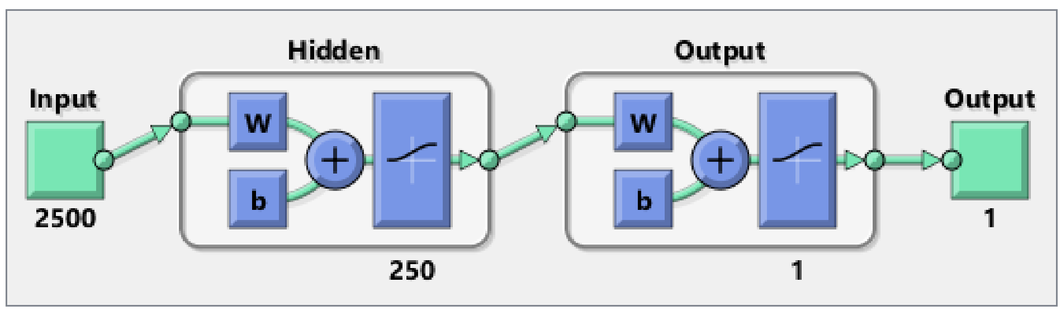


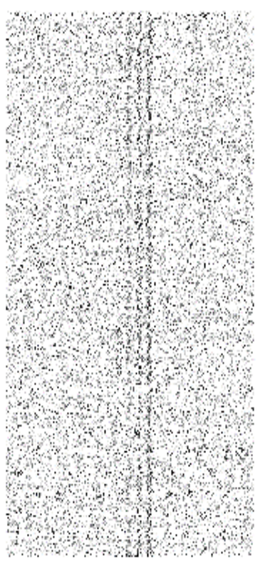


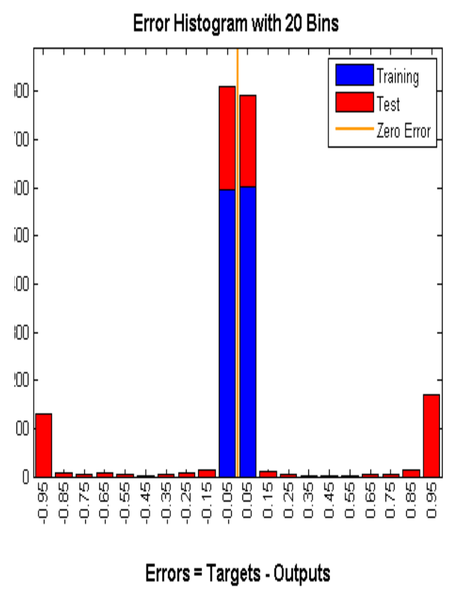




Anonymity Analysis







Rate	DUD			DAD			CAD		
	α	**β**	d(**α**,**β**)	**α**	**β**	d(**α**,**β**)	**α**	**β**	d(**α**,**β**)
0.05	0.499	0.494	0.0001	0.508	0.504	0.0004	0.442	0.426	0.0507
0.1	0.521	0.516	0.0004	0.517	0.511	0.0023	0.472	0.468	0.0104
0.15	0.481	0.474	0.0058	0.491	0.486	0.0015	0.471	0.461	0.0134

References

[1] A. Gurjar and A. Patil, "Cluster based anonymization for source location privacy in wireless sensor network," in *Communication Systems and Network Technologies (CSNT), 2013 International Conference on*, April 2013, pp. 248–251.

[2] M.MahmoudandX.Shen,"Acloud-basedschemeforprotectingsource- location privacy against hotspot-locating attack in wireless sensor networks," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 10, pp. 1805–1818, Oct 2012.

[3] R. Manjula and R. Datta, "An energy-efficient routing technique for pri- vacy preservation of assets monitored with wsn," in *Students' Technology Symposium (TechSym), 2014 IEEE*, Feb 2014, pp. 325–330.