IPHV2I10020X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .1
ISSN Online: 2319 – 9253
Print: 2319 – 9245

A SURVEY ON ROBUST TRUST-AWARE ROUTING FRAMEWORK FOR DYNAMIC WIRELESS SENSOR NETWORKS

P.JayaKrishna[1] , T.Narender[2]

1. M.Tech (CS) , Dept. of Computer Science & Engineering, VITS(N6), Karimnagar.

2. Assistant Professor, Dept. of Computer Science & Engineering, VITS(N6), Karimnagar.

ABSTRACT

Wireless sensor networks are saturated networks because of its usage in our regular life. The protection against the senor networks is very limited. So many attacks like Sybil, wormhole, sinkhole attacks etc. are ready to damage the systems of routers. We are having cryptographic techniques to handle these attacks with trust-aware routing protocol but does not deals with multi-hop routing. We proposed to implement TARF in dynamic wireless network environment and multi-hop routing also.

Keyterms: wireless sensor networks, attacks, TARF, Energy watchers.

Introduction

A wireless sensor network (WSN) is a network made of numerous small independent sensor nodes. The sensor nodes, typically the size of a 35 mm, are self-contained units consisting of a battery, radio, sensors, and a minimal amount of on-board computing power. The nodes self-organize their networks, rather than having a pre-programmed network topology. Because of the limited electrical power available, nodes are built with power conservation in mind, and generally spend large amounts

The devices are also called motes and are intended to shrink down to the size of a grain of sand, or even a dust particle. Each device contain sensors, computing circuits, bidirectional wireless communications technology and a power supply. Motes would gather data, run computations and communicate using two-way band radio with other motes at distances approaching 1,000 feet (300 metres).

When clustered together, they automatically create highly flexible, low-power networks with applications ranging from climate control systems to entertainment devices that interact with information appliances.

Industrial automation uses different kinds of sensors such as sensors for temperature

sensing and control, pressure sensing, level sensing and machinery monitoring.

Environmentalist uses them for environmental monitoring to measure air and water quality as well as seismic activity, health specialist uses them for tele-health monitoring and diagnostics where they significantly reduce overall medical costs by enabling home-based proactive monitoring and medical care, like personalized patient-based monitoring techniques for measuring the heart rate or respiration .

The application of their operation includes building controls (fire alarms systems), thermo technology climate control systems, in military for tracking and monitoring borders and so on. This shows that the content of transmitted data covers a spectrum of applications from low security like thermo technology to the high security requirement for military purposes

This concept of ad hoc networks -- formed by hundreds or thousands of motes that communicate with each other and pass data along from one to another -- is extremely powerful. Here are several examples of the concept at work:

Imagine a suburban neighborhood or an apartment complex with motes that monitor the water and power meters (as described in the previous section). Since all of the meters (and motes) in a typical neighborhood are within 100 feet (30 meters) of each other, the attached motes could form an ad hoc network amongst themselves. At one end of the neighborhood is a super-mote with a network connection or a cell-phone link. In this imagined neighborhood, someone doesn't have to drive a truck through the neighborhood each month to read the individual water or power meters -- the motes pass the data along from one to another, and the super-mote transmits it. Measurement can occur hourly or daily if desired.

A farmer, vineyard owner, or ecologist could equip motes with sensors that detect temperature, humidity, etc., making each mote a mini weather station. Scattered throughout a field, vineyard or forest, these motes would allow the tracking of micro-climates.

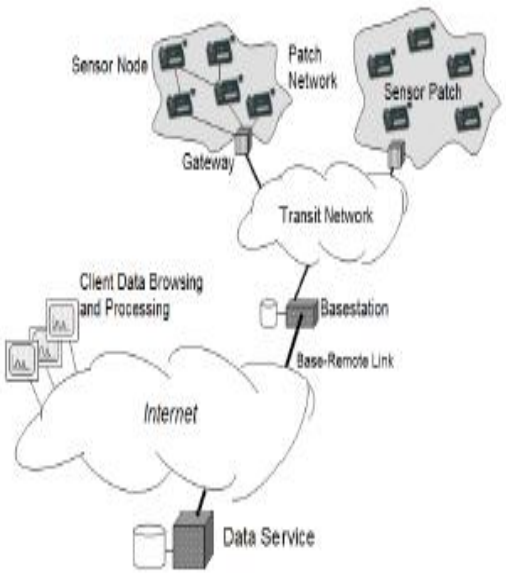
A building manager could attach motes to every electrical wire throughout an office building. These motes would have induction sensors to detect power consumption on that individual wire and let the building manager see power consumption down to the individual outlet.

IPHV2I10020X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .1
ISSN Online: 2319 – 9253
Print: 2319 – 9245

If power consumption in the building seems high, the building manager can track it to an individual tenant. Although this would be possible to do with wires, with motes it would be far less expensive.

A biologist could equip an endangered animal with a collar containing a mote that senses position, temperature, etc. As the animal moves around, the mote collects and stores data from the sensors. In the animal's environment, the biologists could place zones or strips with data collection motes. When the animal wanders into one of these zones, the mote in the collar would dump its data to the ad hoc network in the zone, which would then transmit it to the biologist.

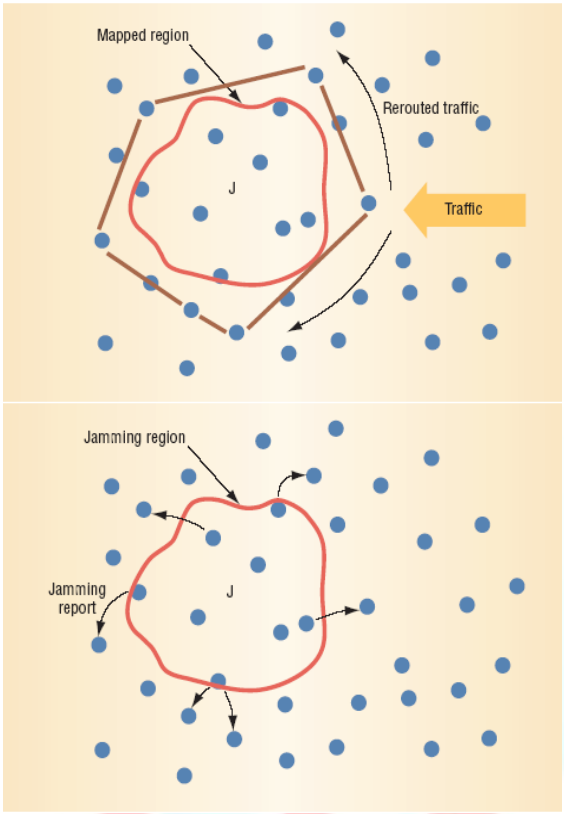
Motes placed every 100 feet on a highway and equipped with sensors to detect traffic flow could help police recognize where an accident has stopped traffic. Because no wires are needed, the cost of installation would be relatively low.



Security Threats

- Denial of Service.
- Spoofed, altered, or replayed routing info.
- Selective forwarding.
- Sinkhole attacks.
- Sybil attacks.
- Wormhole attacks.
- Hello flood attacks.
- Acknowledgement spoofing.

IPHV2I10020X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .1
ISSN Online: 2319 – 9253
Print: 2319 – 9245



Defense Against Jamming

Sybil Attack

- An adversary node assumes identity of multiple nodes.
- This causes ineffectiveness in a network. Specially target for networks with:
  - Fault Tolerance
  - Geographic routing protocol

Wormhole Attack

- Two powerful adversary nodes placed in two strategic location
- Advertise a low cost path to the sink
- All nodes in the network are attracted to them looking for an optimal route
- This is attack is usually applied in conjunction with selective forwarding or eavesdropping attack.

EXISTING MODEL

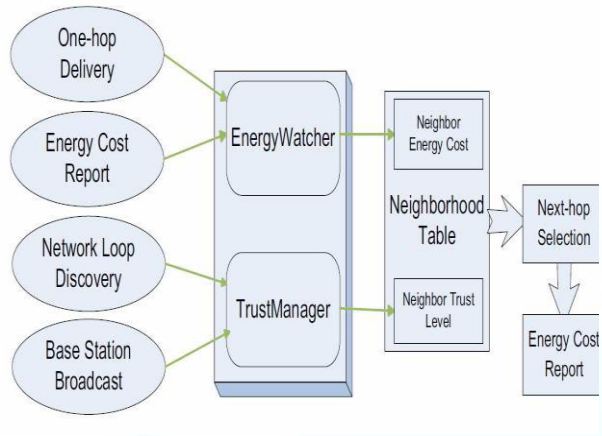
In Existing system, when the file send from base station in that situation hackers aggravated network conditions. A traditional cryptographic techniques effort does not address the severe problems. That time the file could be affected by hackers. So, the network will be damaged. An attacker may tamper nodes physically, create traffic collision with seemingly valid transmission, drop or misdirect messages in routes, or jam the communication channel by creating radio interference.

PROPOSED MODEL

In Proposed System, focuses on the kind of attacks in which adversaries misdirect network traffic by identity deception through replaying routing information. Based on identity deception the adversary

IPHV2I10020X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .1
ISSN Online: 2319 – 9253
Print: 2319 – 9245

is capable of launching harmful and hard to detect attacks against routing, such as selective forwarding, wormhole attacks, sinkhole attacks, and Sybil attacks.



PRAPOSED MODULES

1. ROUTING THE NETWORK

2. TRANSFER FILE

3. SINKHOLE AND WORMHOLE ATTACKS

4. ENERGY WATCHER & TRUST MANAGER

ROUTING THE NETWORK:

In this module, the networks embedded on the physical fiber topology. However, assessing the performance reliability achieved independent logical links can share the same physical link, which can lead to correlated failures. Mainly, we focus on assessing the reliability of energy level and trusted network.

TRANSFER FILE

In this module, Analysis the Shortest Path algorithm independently routes each logical link on a physical path with the minimum number of hops in trusted network basis. Since we are assuming that every physical link fails with the same probability, the failure probability of path is minimized when it is routed over the shortest path. Hence, under the algorithm Shortest Path, each light- path greedily takes the most reliable route and transfers the file.

SINKHOLE AND WORMHOLE ATTACKS

Prevent the base station from obtaining complete and correct sensing data

- Particularly severe for wireless sensor networks
- Some secure or geographic based routing protocols resist to the sinkhole attacks in certain level
- Many current routing protocols in sensor networks are susceptible to the sinkhole attack
- Set of sensor nodes
  - continuously monitor their surroundings
  - forward the sensing data to a sink node, or base station

- Many-to-one Communication
  - Vulnerable to the sinkhole attack, where an intruder attracts surrounding nodes with unfaithful routing information
  - Alters the data passing through it or performs selective forwarding.

ENERGY WATCHER & TRUST MANAGER:

In this module Cluster-based WSNs allows for the great savings of energy and bandwidth through aggregating data from children nodes and performing routing and transmission for children nodes. In a cluster-based WSN, the cluster headers themselves form a sub-network, after certain data reach a cluster header, the aggregated data will be routed to a base station only through such a sub network consisting of the cluster headers. Our framework can then be applied to this sub-network to achieve secure routing for cluster based WSNs. Trust Manager encourages a node to choose another route when its current route frequently fails to deliver data to the base station. Though only those legal neighboring nodes of an attacker might have correctly identified the adversary.

CONCLUSION

Wireless sensor network is a growing field and has many different applications. Most security threats to wireless ad-hoc network are applicable to wireless sensor network. These threats are further complicated by the physical limitations of sensor nodes. Some of these threats can be countered by encryption, data integrity and authentication. Security is achieved through TAR's in multi-hop routing systems effectively and handle the attacks successfully.

REFERENCES

[1] G. Zhan, W. Shi, and J. Deng, "Tarf: A trust-aware routing framework for wireless sensor networks," in *Proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN'10)*, 2010.

[2] F. Zhao and L. Guibas, *Wireless Sensor Networks: An Information Processing Approach*. Morgan Kaufmann Publishers, 2004.

[3] A. Wood and J. Stankovic, "Denial of service in sensor networks,"*Computer*, vol. 35, no. 10, pp. 54–62, Oct 2002.

[4] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks:

attacks and countermeasures," in *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, 2003.

[5] M. Jain and H. Kandwal, "A survey on complex wormhole attack in wireless ad hoc networks," in *Proceedings of International Con-ference on Advances in Computing, Control, and Telecommunication Technologies (ACT '09)*, 28-29 2009, pp. 555 –558.

[6] I. Krontiris, T. Giannetsos, and T. Dimitriou, "Launching a sinkhole attack in wireless sensor networks; the intruder side," in *Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications(WIMOB '08)*, 12-14 2008, pp. 526 –531.

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis and defenses," in *Proc. of the 3rd International Conference on Information Processing in Sensor Networks (IPSN'04)*, Apr. 2004.

[8] L. Bai, F. Ferrese, K. Ploskina, and S. Biswas, "Performance analysis of mobile agent-based wireless sensor network," in *Proceedings of the 8th International Conference on Reliability, Maintainability and Safety (ICRMS 2009)*, 20-24 2009, pp. 16 –19.

[9] L. Zhang, Q. Wang, and X. Shu, "A mobile-agent-based middleware for wireless sensor networks data fusion," in *Proceedings of Instrumentation and Measurement Technology Conference (I2MTC '09)*, 5-7 2009, pp. 378 –383.

[10] W. Xue, J. Aiguo, and W. Sheng, "Mobile agent based moving target methods in wireless sensor networks," in *IEEE International Symposium on Communications and Information Technology (ISCIT 2005)*, vol. 1, 12-14 2005, pp. 22 – 26.

[11] J. Hee-Jin, N. Choon-Sung, J. Yi-Seok, and S. Dong-Ryeol, "A mobile agent based leach in wireless sensor networks," in *Proceed- ings of the 10th International Conference on Advanced CommunicationTechnology (ICACT 2008)*, vol. 1, 17-20 2008, pp. 75 –78.

[12] J. Al-Karaki and A. Kamal, "Routing techniques in wireless sensor networks: a survey," *Wireless Communications*, vol. 11, no. 6, pp.6–28, Dec. 2004.