Candidate Base Stations a Security Solution For Compromised Base Stations In Wireless Sensor Networks

Nabaasa Evarist
College of Computer and Communication, Hunan University, P. R. China
nabaasa_kyo@yahoo.com

Yaping Lin
College of Computer and Communication, Hunan University, P. R. China
yplin@hunu.edu.cn

ABSTRACT

Wireless sensor networks heavily rely on base stations for data processing and routing within the network itself and the outside world. Considerably less attention has been put on the security of base stations in comparison with sensor nodes, simply because the base stations are expected to be secure enough not to be attacked or even be compromised. In this research paper we propose, Candidate Base Stations, base station failure detection, in which the sensor network should be able to automatically and promptly resort to a candidate base station, which takes over the roles of a compromised base station. Our strategy of candidate base stations, tries to ensure presence of the same number of base stations on the network even after some have been compromised. With candidate base stations, base station security is more guaranteed, our experimental results indicate a greater secure network with this scenario.

Key words: wireless sensor networks, base station, candidate base station, sensor node, ns-2

1. 0 Introduction

A wireless sensor network (WSN) is a network made of numerous small independent sensor nodes. The sensor nodes 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.

Candidate base stations, are base stations with similar characteristics as the currently active base stations, they only play base station roles when they are resorted to (i.e. when there is a base station compromise/failure) otherwise they just pretend to be ordinary nodes on the sensor network. Candidate base stations are very vital, since they ensure prolonged base station security and availability on the network. They greatly increase network resilience and enhance fault tolerance.

Prior sensor network researches have always assumed that base stations are secure enough not to be attacked or even be compromised [6] and hence researchers have always concentrated on enhancing security for sensor nodes [4] which rely on base stations hoping that base stations will always be available and never compromised. Base stations can be attacked and even compromised like any other sensor node on the network. Some strategies for enhancing base station security have been proposed [7], however those strategies do not give room for replacing a possibly compromised base station, they only advocate for fault tolerance whereby sensor nodes resort to the possibly remaining base stations on the network in case a base station is compromised.

Because of lack of candidate base stations in the current base station security protocols available for wireless sensor networks, we are venturing into this idea of incorporating candidate base stations in order to realize highly increased base station security. The rest of the paper is organized as follows: Section 2 briefly elaborates the current and the proposed base station security protocols. In section 3, we give detailed

discussion of our proposed model and the assumptions. Section 4 we discuss the simulation results. In section 5 we look at the future work and finally in section 6 we conclude our research topic.

2.0 Network Architecture and Base Station Security Protocols

2.1 Related work.

Currently, base stations in wireless sensor networks do solely support themselves due to the network layout structure available and the security protocols under use. There are just stand-alone base stations in the multi-layered network infrastructure.

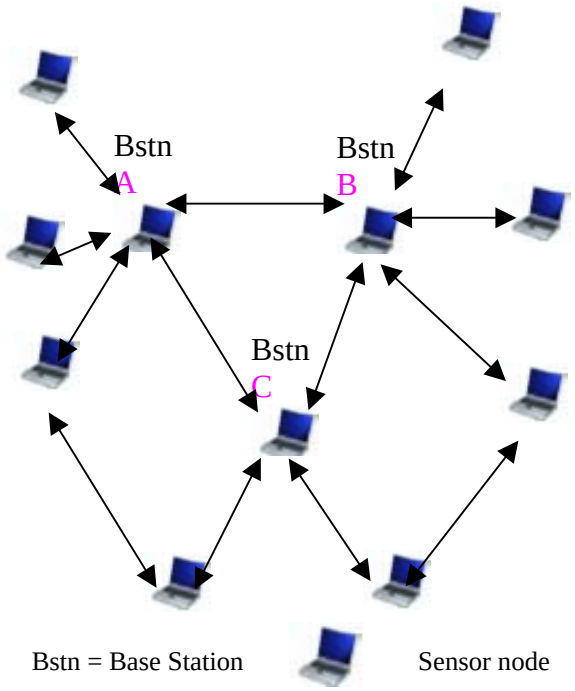

Figure 1: Multi-layered network infrastructure

In figure 1 above, the base station security protocols entirely assume that, once any base station is compromised, then sensor nodes that have been processing and routing their data through that compromised base station have to process and re-route their traffic via any other remaining base station on the network. INSENS (INtrusion-tolerant routing protocol for wireless SEnsor NetworkS) [6] has several important useful features, it suffers from a serious drawback. It assumes that the base station cannot fail or be isolated from the network by malicious compromised nodes. This assumption may not hold under several scenarios. For example, if an adversary discovers the location of a base station, it can isolate it from the rest of the network by simply jamming the communication medium in its neighborhood. In this protocol, base stations can be greatly reduced provided the adversary persists with attacks on the remaining base stations.

2.2 Base Station Security protocol with Candidate Base Stations.

In order to ensure failure resistant, increase resilience and fault tolerance on the network, each base station is supported by a candidate base station (CBs). Each candidate base station is within the same domain as its master i.e. the currently running base station and the corresponding sensor nodes.

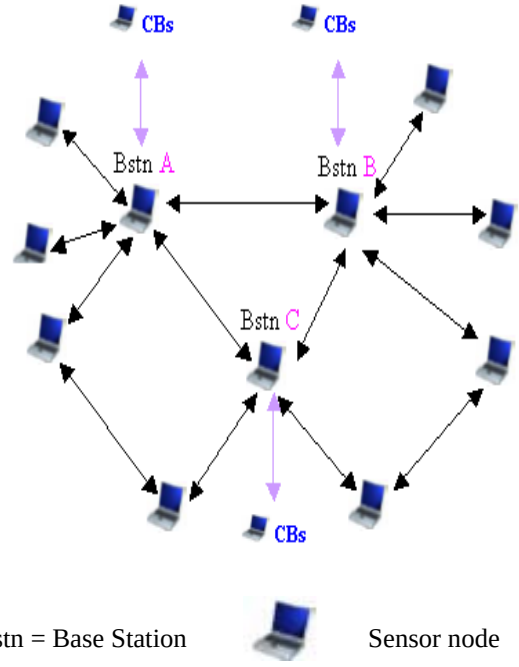

Figure 2: Multi-layered network infrastructure with Candidate Base Stations

The network infrastructure model presented in figure 2 above introduces candidate base stations to the base station security protocols and embraces the multiple base stations security protocol as advocated by other already available security protocols like INSENS. With candidate

base stations and multiple base stations available in our proposed base station security protocol, we believe the security of the base station on the wireless sensor network will be greatly improved. However, we need to establish good mechanisms by which sensor nodes are able to quickly detect and invoke a CBs and also we need to find out the challenges of introducing candidate base stations on the entire wireless sensor network.

3.0 Candidate Base Stations

Candidate base stations are a good means of supporting the existing base stations in case of any compromise. With candidate base stations, network segmentation, paralysis and data loss are greatly minimized since they quickly take over the roles of the possibly compromised base stations. They also help in reducing the big workload that would otherwise be exerted on the fewer remaining base stations because candidate base stations take over the entire set of roles that the compromised base station was playing on the network and so these roles do not have to be met by the other remaining base stations.

In our proposed candidate base station model, we have some assumptions: - one candidate base station for each base station, candidate base stations have the same characteristics as their master base stations, before base station failure candidate base stations are known to be just normal sensor nodes by other sensor nodes, the base station knows its CBs and updates it periodically.

3.1 Candidate Base Station Model

The candidate base station model is fitted in the base station security protocol at the network layer with links to the link layer and the application layer. In this way, the security protocol is made more stable right away from the initial stages of data auditing and routing on the wireless sensor network.

Unlike other base station security protocols, candidate base station security protocol advocates for detection of possibly compromised base station(s). The main reason for detecting compromised base station(s) is that, the CBs security protocol tries to quickly invoke the candidate base station to take over the role of the compromised base station such that the same number of base stations is maintained on the network. If it happens that, the CBs is compromised first and then later the base station is also compromised, then the protocol reduces to the same protocols that do not embrace candidate base stations i.e. the nodes have to just resort to the possibly remaining base stations on the network. The scenario of candidate base stations, gives more complexity to the adversary

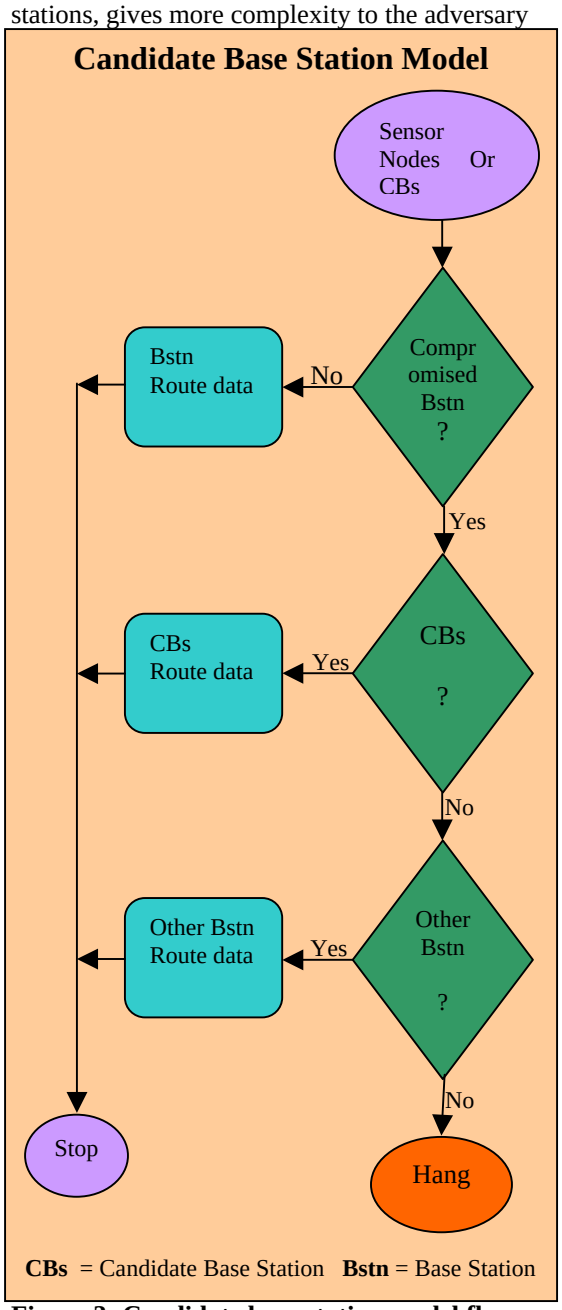

Figure 3: Candidate base station model flow diagram

who must first discover the location of the hidden CBs and all its traditional security guards before he/she can be able to compromise it and then, the adversary still has the task of

compromising the base station too, all this to execute his/her mission well, still the problem of the compromised base station is localized, increases on the impossibility of the adversary achieving the mission. If the adversary is successful, it cannot affect the entire network since the protocol also embraces multiple routing.

Figure 3 above shows the display of the candidate base station model, the chart shows the flow of decisions that need to be made and how the presence of candidate base stations helps to avoid paralysis, segmentation of the network due to one or more base station failure.

Candidate base station model as depicted in figure 3 above, serves to highly mandate and improve the security of the base station. There are seven main modules in it: -

3.2 Sensor nodes or CBs module

The wireless sensor network is arranged into different domains that contain designated sensor nodes, the CBs and the currently running base station. This module handles the information about the number of sensor nodes, CBs, plus the base station, which are available in a particular domain. Each domain contains several number of sensor nodes, a CBs and a base station. This arrangement is hierarchical in a way that, the network is arranged in domains, clusters and the communication paradigm is from node to base station, node to node, and vice versa.

Algorithm: Given a wireless sensor network with d domains, each domain containing b_i base stations, c_i candidate base stations, n_i sensor nodes, and if bcn_i is the sum of the number of base stations plus candidate base stations plus sensor nodes, in a particular **i-th** domain then: -

$$bcn_i = b_i + c_i + n_i \ , \ 1 \le i \le d$$

But $\forall i, 1 \le i \le d$, $b_i = 1$ and $c_i = 1$, since we assume that every domain contains only one base station and for every base station there exists only one candidate base station, hence: -

$$bcn_i = 1 + 1 + n_i \ , \ 1 \le i \le d$$

$$bcn_i = 2 + n_i \ , \ 1 \le i \le d$$, therefore the total number of base stations plus candidate base stations plus sensor nodes for the entire network is given by: -

$$\sum_{i=1}^{i=d} bcn_i$$

3.3 Compromised base station module

It is the sole responsibility of the sensor nodes (usually the cluster heads) or the candidate base station within a particular domain to find out whether their corresponding base station has been compromised or not. In this module the sensor nodes or the hidden CBs which are usually one hope away from the base station, keep on polling the base station purposely to find out whether its still alive. In our security protocol, we let the polling agents wait for a specified period of time k, to elapse before they can really confirm that the base station has been compromised. If no base station failure then data is normally processed and routed by the base station, otherwise a CBs module has to be invoked.

Algorithm: Given m_i as the normal sensor nodes just one hope away from the base station within the **i-th** domain then, $m_i + c_i$ is the total number of communicating agents just one hope away from the actual base station, because we assumed that c_i is always just one hope away from its master base station too and we know that $c_i = 1$. Therefore, the base station always receives polling messages from the $m_i + 1$ surrounding agents (sensor nodes and the hidden candidate base station) to find out whether its working normally or not. If any of the $m_i + 1$ agents discovers base station failure, i.e. after waiting for a specified k period of time (the best k still remains a topic of interest), then it triggers candidate base station invoking module, in which requests to invoke a candidate base station into a new base station are sent out to the remaining agents among which we expect to find the candidate base station.

3.4 Candidate base station module

Within the candidate base station module, the process of invoking the CBs is executed. After one or more sensor nodes or CBs discovering base station failure, the process of discovering the CBs starts. It should be noted that, the CBs is always hidden in such a way that other sensor nodes initially know it as just a normal sensor node in their domain, apart from the base station which always updates it regularly. In this module sensor nodes broadcast amongst themselves in order to discover the CBs which in turn

automatically takes over the roles of the compromised base station and redirects routing protocols of that particular domain through it. The CBs can also discover base station failure first, in which case it invokes itself into the new base station and broadcasts to the other sensor nodes within that domain about the new changes.

Algorithm: If any of the $\mathbf{m_i}$ discovers base station failure, it immediately starts sending candidate base station invoking requests to any of the $\mathbf{n_i}$ + $\mathbf{c_i}$ nodes, until it receives a confirmation reply from $\mathbf{c_i}$, at which point $\mathbf{c_i}$ automatically takes over the role of the base station and broadcasts to all $\mathbf{n_i}$ sensor nodes in that domain on the network for the changes. If $\mathbf{c_i}$ discovers base station failure first, it immediately invokes itself into a new base station, then broadcasts to all the $\mathbf{n_i}$ sensor nodes via some or all of the $\mathbf{m_i}$ nodes for the new changes. The process of invoking a CBs into a new base station, involves updating of the candidate base station routing tables and election of the new nodes that are one hope away from the new base station, these nodes will include all or some of the old $\mathbf{m_i}$'s.

3.5 Other base station module

In case the CBs is not available and yet the base station has been compromised, then the entire candidate base station security protocol in a given domain, reduces to the same base station security protocols that just rely on any other possible remaining base station on the network. In this module multiple routing techniques are employed to ensure quick discovery of the less costly base station that can be resorted to for data processing and routing. Although as would be expected, there is more cost of time, data loss and constraint of other network resources before discovering any other remaining base station in other domains, unlike in the presence of a CBs whereby such costs are tremendously reduced. Absence of *any other base station* triggers that part of the network to invoke the hang module.

Algorithm: Since the base station has been compromised and the CBs is not available (possibly having been compromised also), then $\mathbf{bcn_i} = \mathbf{n_i}$. It should be noted that, $\mathbf{n_i}$ includes $\mathbf{m_i}$. Any of the $\mathbf{n_i}$ can send "*Any Other base station Requests*" to the remaining $\boldsymbol{d}$-1 domains to have its data processed and routed by the base station in that domain accordingly. This process involves determination of the least expensive base station in terms of network resources. These requests are sent for a specified period of time, after which if there is no positive response then, the requesting sensor node invokes the "*Hang module*".

3.6 Route data module

In this module, it is either the base station, the CBs or *any other base station* (in another domain) that will do the processing and routing of the data depending on the current state of the base station in a given domain. If there is no base station failure then, the base station functions normally, otherwise it's the CBs to do the data processing and routing.

3.7 Hang module

When this module is executed, it indicates total success of the adversary having managed to fail the base station and the CBs and no route to *any other base station* in other domains. In this state, an adversary has rendered the network or part of the network vulnerable and incapacitated due to the failure of the base station(s). The communicating sensor node is made to stop data forwarding. This situation can lead to network segmentation and paralysis. However since our proposed protocol embraces multiple routing too, we believe this state is very hard to attain.

3.8 Stop module

This module just confirms that, the base station security protocol of the network is still working, data is successfully processed and routed well, irrespective of whether a certain base station having been compromised or not.

4.0 Simulation Set-up and Discussion

To evaluate our approach, we implement our candidate base station security protocol in the ns-2 network simulator [10]. The simulations contain 160 non-mobile wireless sensor nodes in 1000m x 1000m area for 600 seconds in simulation time. In all simulations, pause time is set to either 0 or 10 seconds and maximum speed to 0, 1, 5, 10, and 20 m/s. The number of base stations and candidate base stations in the network varies among 1, 3, 4, 8, 10, 11, 12, 15 and 16. For the detection and candidate base station invoking process, 100 non base station nodes (i.e. candidate base stations and sensor nodes, usually cluster heads) each makes 10 base station failure and candidate base station

invocation requests randomly distributed over the whole simulation, which add up to a total of 1000 requests during 600 seconds. This is roughly 100 requests per minute, on average we are convinced to believe that, this is a reasonable number.

4.1 Base Station Failure Detection

Due to the need of knowing how many base stations still exist on the network and what impact do the compromised base stations have on the entire network, we carried out experiments with varying number of compromised base stations with varying number of candidate base stations too. The entire network contains 16 base stations and automatically this implies 16 candidate base stations present, since from the beginning we assumed that each base station has only one corresponding candidate base station to boost up its security. Since the entire network is hierarchical and arranged in domains, each domain contains only one base station and one candidate base station.

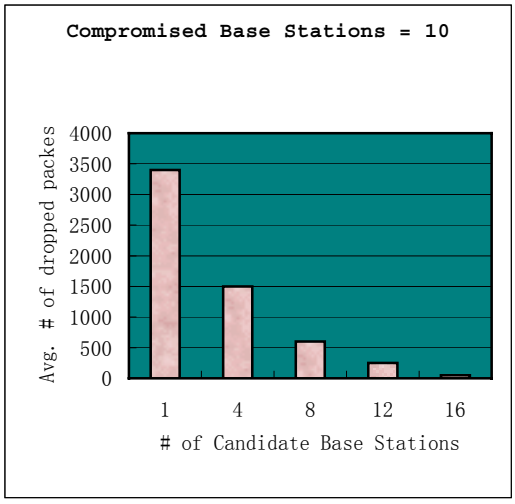

Figure 4: Candidate Base Stations Vs. Dropped Packets

In figure 4 above, we display the results of 10 compromised base stations with varying number of available candidate base stations on the network while monitoring the average number of dropped packets from different communicating nodes between the time of base stations failure up to the time of candidate base station election. Considerably with presence of only one CBs, the number of dropped packets is so high compared to when there is an increased number of available candidate base stations, for instance, with 16 candidate base stations and given 10 compromised base stations, the number of dropped packets is just in *tens* which is far away small compared with just one candidate base station available where the number of dropped packets is in few thousands. The number of dropped packets can easily vary depending on the number of communicating nodes and the speed of communication amongst the nodes, but the prime fact is that, with more candidate base stations present, the possible number of dropped packets is greatly reduced compared to when there are very few or no candidate base stations present.

4.2 Candidate Base Station Success Ratio

From all the simulations, a communicating agent gets back more than (4/5) of the candidate base station invocation request replies from a particular CBs being invoked. This average holds throughout the varying scenarios with different number of candidate base stations and different network topological settings. Figure 5 below, shows the distribution of successfully received candidate base station invocation request replies. Our protocol maintains almost a constant distribution under different network topologies with increasing number of candidate base stations. The more the candidate base stations present, the more the success ratio of the received replies. We believe that this is because of the effectiveness of the robust candidate base stations which have exactly the same characteristics as their master base stations and so they have a high ability to respond quickly to the requesting nodes since there computational power is far much higher than the ordinary sensor nodes.

The candidate base station success ratio indicates the ability/chance of invoking hidden CBs by a requesting communicating agent that discovered a possibly compromised Bstn. This experiment considered different speeds of data communication between the CBs and the requesting agent. At different speeds, it was observed that, the request replies received from the CBs being invoked are approximately constant and usually above (4/5), however there is tremendous increase in the successful request replies received as the number of candidate base station increases.

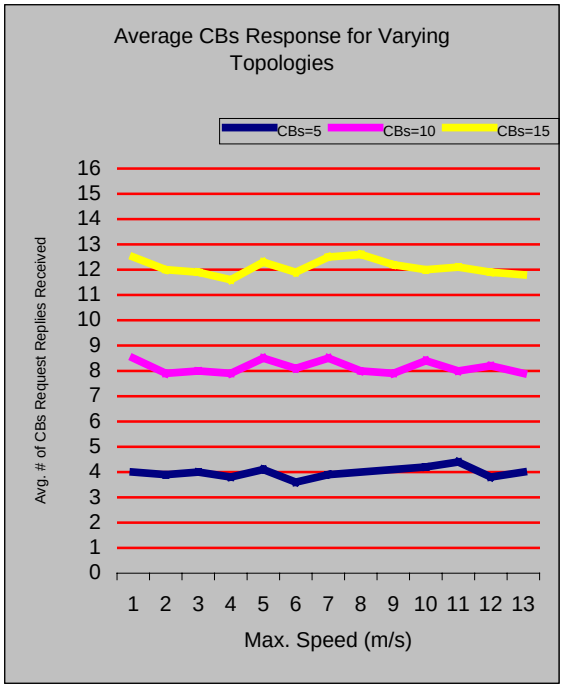

Figure 5: Success Ratio of CBs Request Replies

Different candidate base stations were supplied in the network (i.e. 5, 10, and 15) such that, the entire network is well observed in terms of success ratios of the number of request replies received. By observing the figure above, it can easily be noted that, the more the candidate base stations are proportional to the compromised base stations the better the success ratio, hence verifying our protocol strategy of one candidate base station for every base station to be effective and more reliable. It should be noted that, the number of candidate base stations invoked always depended on the number of compromised base stations.

4.3 Disconnected Sensor Nodes

In the following experiment, all the 16 base stations were compromised within the first 200 seconds into the total execution time of the entire experiment (i.e. 600 seconds). These 16 base stations were compromised randomly one after the other with some random time lag in between while different number of candidate base stations were present and invoked. In this scenario we tried to observe the number of sensor nodes that would be completely or temporary disconnected from the rest of the network

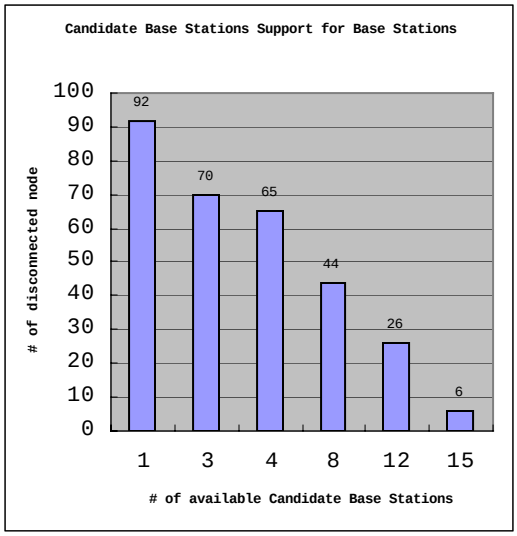

Figure 6: CBs Vs. Disconnected nodes

With only 1 candidate base station present and having compromised 16 base stations randomly and at different times but within the first 200 seconds of the entire experimental running time (i.e. 600 seconds), it was observed that 92 sensor nodes out of the 160 available sensor nodes were disconnected. With exactly the same set up but only varying the number of candidate base stations, great improvements were achieved. For instance from figure 6 above, we note that, with 8 candidate base stations available the number of disconnected nodes greatly reduced to only 44, while on even a more remarkeable side with 15 candidate base stations present (note, having compromised 16 base stations), only 6 nodes were disconnected. This clearly indicates a positive trend whereby, given a particular number of compromised base stations, the more the available candidate base stations are, the less the number of disconnected nodes one can expect to have on the network.

5.0 Future Work

In this research paper we assumed one candidate base station for every base station, the best number of candidate base stations for each base station should be evaluated more. How should a candidate base station get its own candidate base station, is a question that still needs attention and also there is need to know the network overhead introduced due to polling between the base station and the nodes that are trying to find out whether its not yet compromised. When should candidate base station(s) be updated with the data on the base station? Which is the best

location of candidate base station(s) from the base station, in this research we just assumed it to be just one hope away.

6.0 Conclusion

Wireless sensor networks have brought about a paradigm shift in the way we think about base station security assurance. There is total need to rethink methods for these new networks based on the characteristics that they have. In this paper, we have provided an over view of wireless sensor networks. We then proceeded to provide an introduction to base station security protocols in the context of wireless sensor networking. Having understood the implications and problems of the current base station security protocols which do not embrace base station failure detection but just to rely on any other possibly remaining base station on the network, we proposed a candidate base station security model that contains different modules and still embraces the good features of the previously proposed base station security protocols, we performed base station failure detection, we also carried out candidate base station invoking to take over the roles of a possibly compromised base station. All our experiments were done in ns-2 and the results of our model show that, there is higher base station security with the provision of base station failure detection and candidate base station invocation on the wireless sensor network.

REFERENCES

[1] Zhou. L and Haas Z, “Securing Ad Hoc Networks,” IEEE Network Magazine, vol. 13, no. 6, November/December 1999.

[2] A. Mainwaring, J. Polastre, R. Szewczyk D. Culler, J. Anderson, "Wireless Sensor Networks for Habitat Monitoring", First ACM Workshop on Wireless Sensor Networks and Applications (WSNA) 2002, pp. 88-97.

[3] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, "SPINS: Security Protocols for Sensor Networks," Proceedings of Seventh Annual International Conference on Mobile Computing and Networks MOBICOM 2001, July 2001.

[4] J. Staddon, D. Balfanz, G. Durfee, “Efficient Tracing of Failed Nodes in Sensor Networks”, First Workshop on Sensor Networks and Applications, WSNA’02, Atlanta, Georgia, USA.

[5] C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

[6] J. Deng, R. Han and S. Mishra, “The Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks”, to appear in IEEE 2nd International Workshop on Information Processing in Sensor Networks (IPSN '03), Palo Alto, CA, USA, April, 2003.

[7] J. Deng, R. Han and S. Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," Technical Report CU-CS-951-03, Department of Computer Science, University of Colorado, 2003.

[8] S. Slijepcevic, V. Tsiatsis, S. Zimbeck, “On Communication Security in Wireless Ad-Hoc Sensor Networks”, Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), June 2002, Pittsburgh, Pennsylvania, USA.

[9] Edgar H., Jr. Callaway, Edgar H. Callaway, “Wireless Sensor Networks: Architectures and Protocols”, 26 August, 2003

[10] NS2 Web Site, http://www.isi.edu/nsnam/ns.