CS5011 A4

150006108

December 2018

1 Part 1

1.1 BN 1

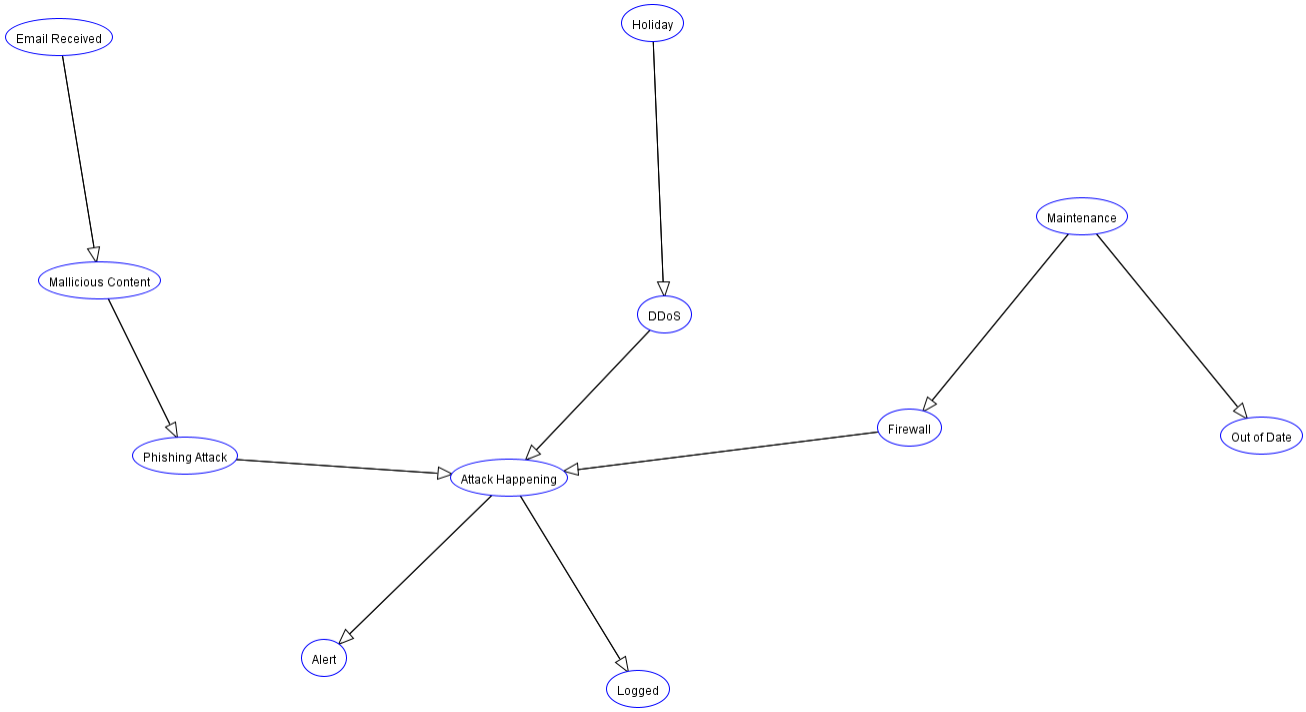

Figure 1: BN 1

Above is the Bayesian Network I designed to display all the features listed in the specification.

The first feature is represented in the left branch. An email is received, with a 75% chance of a it being a business email, and 25% chance of it being personal (this is the domain). When an email has been received, the chance that it contains malicious content is dependent on the type of email received. Given the email is business, there is a 40% chance it will be malicious, whereas if the email is personal, there is a 15% chance it will be malicious. As stated in the specification, business emails have a higher chance of being malicious. If an email is found to malicious, a phishing attack will be occurring, however there is a 3% chance of the detector getting this wrong. As such, there is a 3% chance that the system will either think an attack is

happening when it isn't, or that there isn't an attack happening while there *is*.

The second feature is represented by the right branch. At any given time, I have said there is a 20% chance of maintenance occurring. There is also a 2% chance the recording of the maintenance being out of date, which I interpreted as being somewhat independent to the rest of the system. When maintenance occurs, there is a 5% chance the firewall will be deactivated. However, if no maintenance is occurring, the firewall has a 100% chance of being on.

Feature 3 is represented by the middle branch. We are told there is a $\frac{100}{360}$ chance of any given day being a holiday. This equates to 27.7%. We are also told that DDoS attacks are more common on holidays. As such, the chance of a DDoS attack given the day is a holiday is 40%, whereas the chance of a DDoS attack when it isn't a holiday is only 10%.

Feature 4 is represented with "Attack Happening" and "Alert". The central node contains the CPT relating to all three cases. If the firewall is active, the chance of an attack happening is lowered. If both forms of attack are true at the same time, there is a higher chance of an attack occurring as well. There is also a chance an attack is happening even when both are false, be it one is a false negative, or the system is being attacked from a different avenue. I have interpreted that there is a 20% chance a false alert will be given, as in, an alert will be given even though no attack is happening, or no alert will be given when an attack is detected.

Feature 5 is represented within the "Logged" node. There is a 30% that normal behaviour will be logged as anomalous, and vice versa.

1.2 BN 2

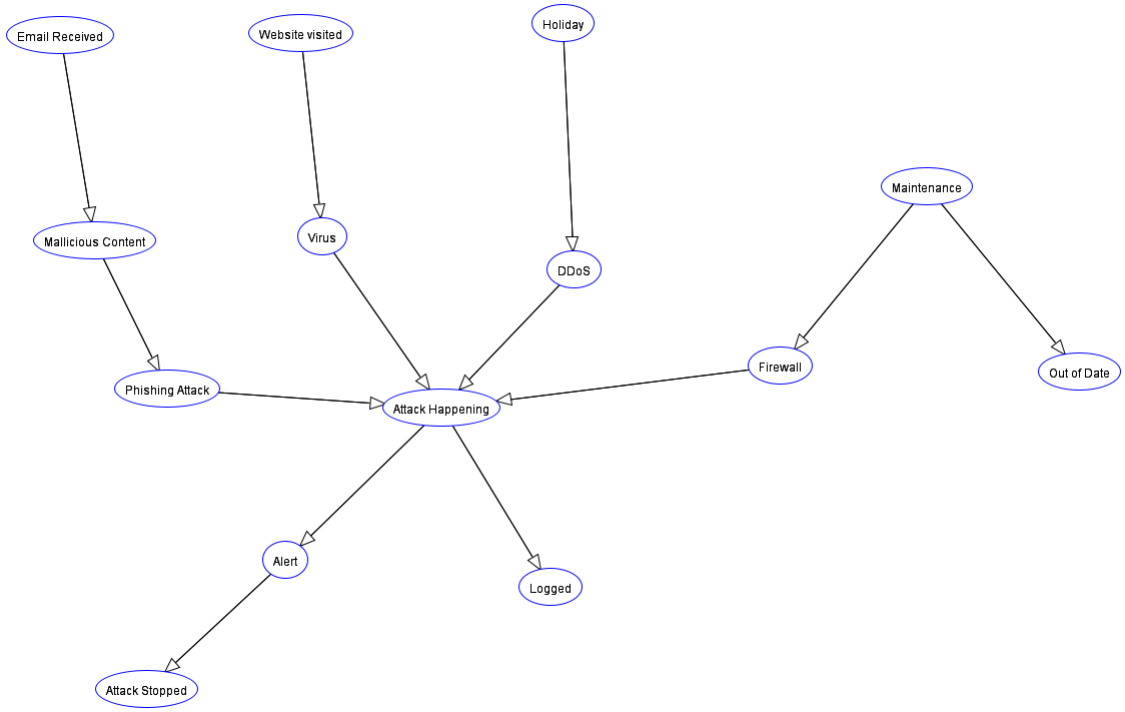

Figure 2: BN 2

The first of the two features I added was introducing the chance for an employee to visit a dangerous website and subsequently effect the system with a virus. I gave them a 10% chance of visiting an infected website. If the website was "dodgey", I said there was a 70% chance of a virus being downloaded, and if it was clean, a 5% chance. The "Attack Happening" node was then updated with the new attack statistics.

The second feature was looking at the chance the attack was stopped given an alert was raised. If an alert was raised, I said there was a 90% chance the attack will be stopped. However, if no alert was raised, there would be a 40% chance the attack was stopped.

1.3 Queries

1.3.1 Diagnostic

With the alert being observed as true, what is the probability it was triggered by a detection of a DDoS attack.

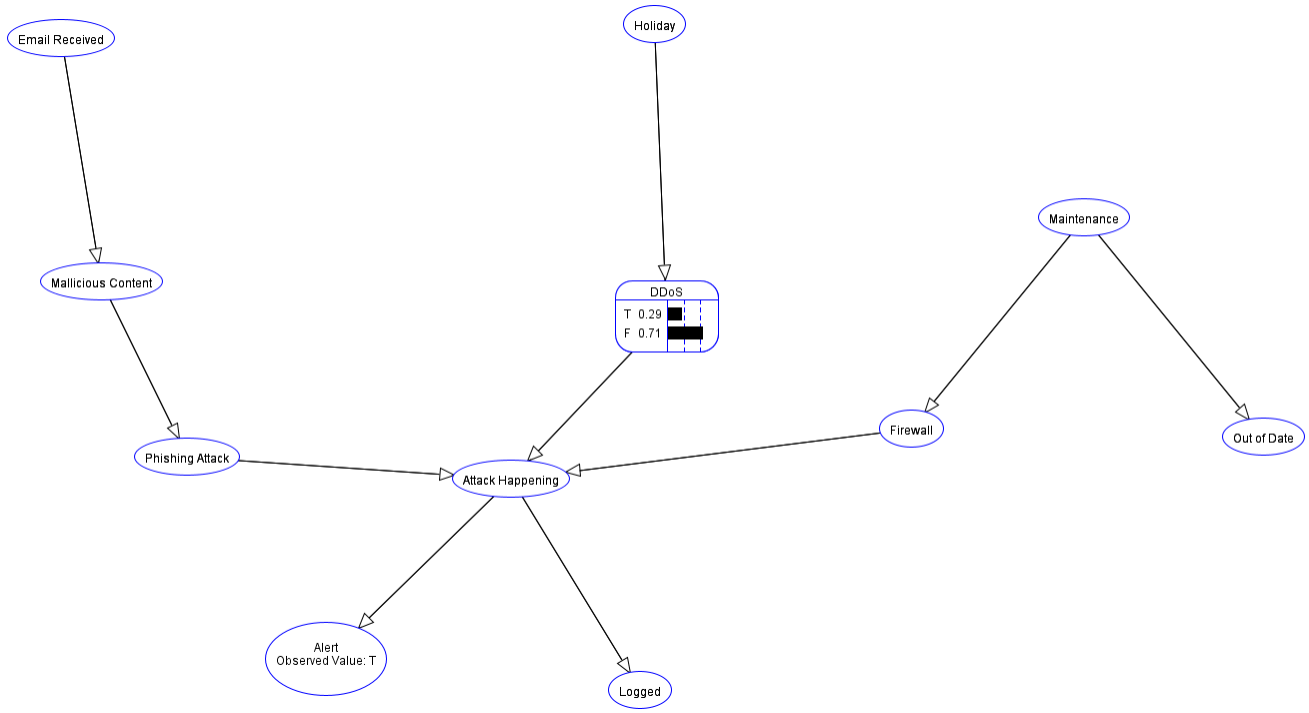

Figure 3: BN 1 Diagnostic query

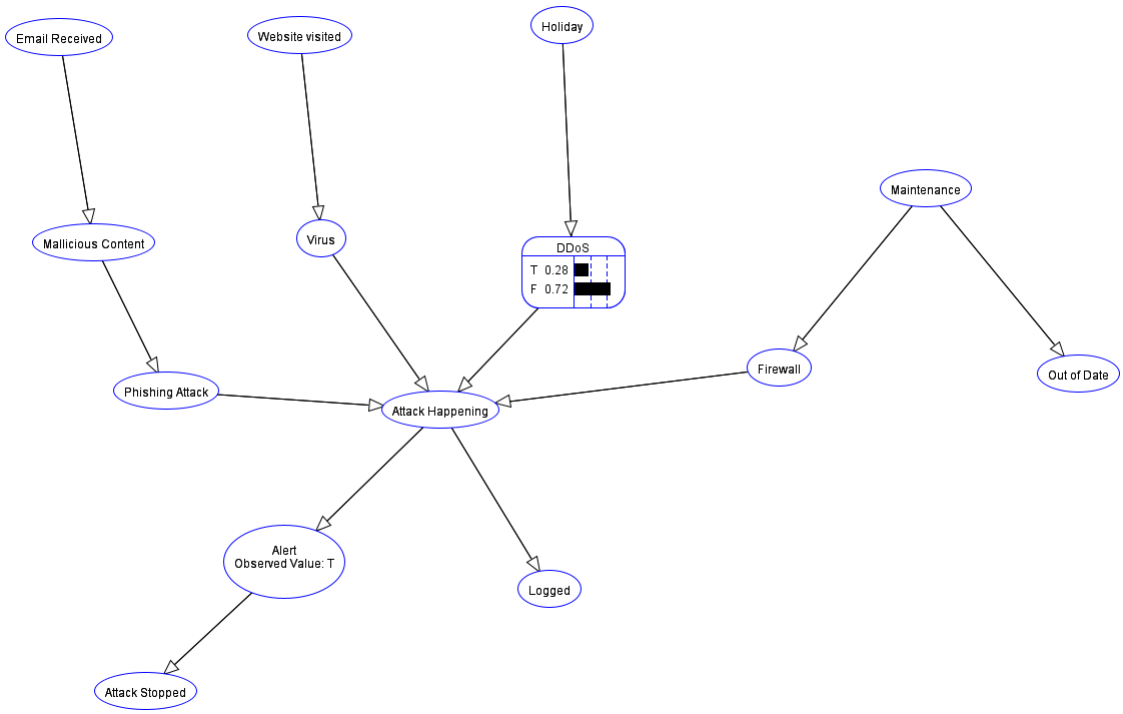

Figure 4: BN 2 Diagnostic query

Here we observe the effects of adding a new form of attack. In BN 1, the chance of a DDoS triggering an alert is given as 29%, whereas in BN 2 it is now 28%, as there is an extra possibility.

1.3.2 Predictive

Given that an email has been received, it is a holiday, and there is maintenance occurring, what are the chances an alert will be raised?

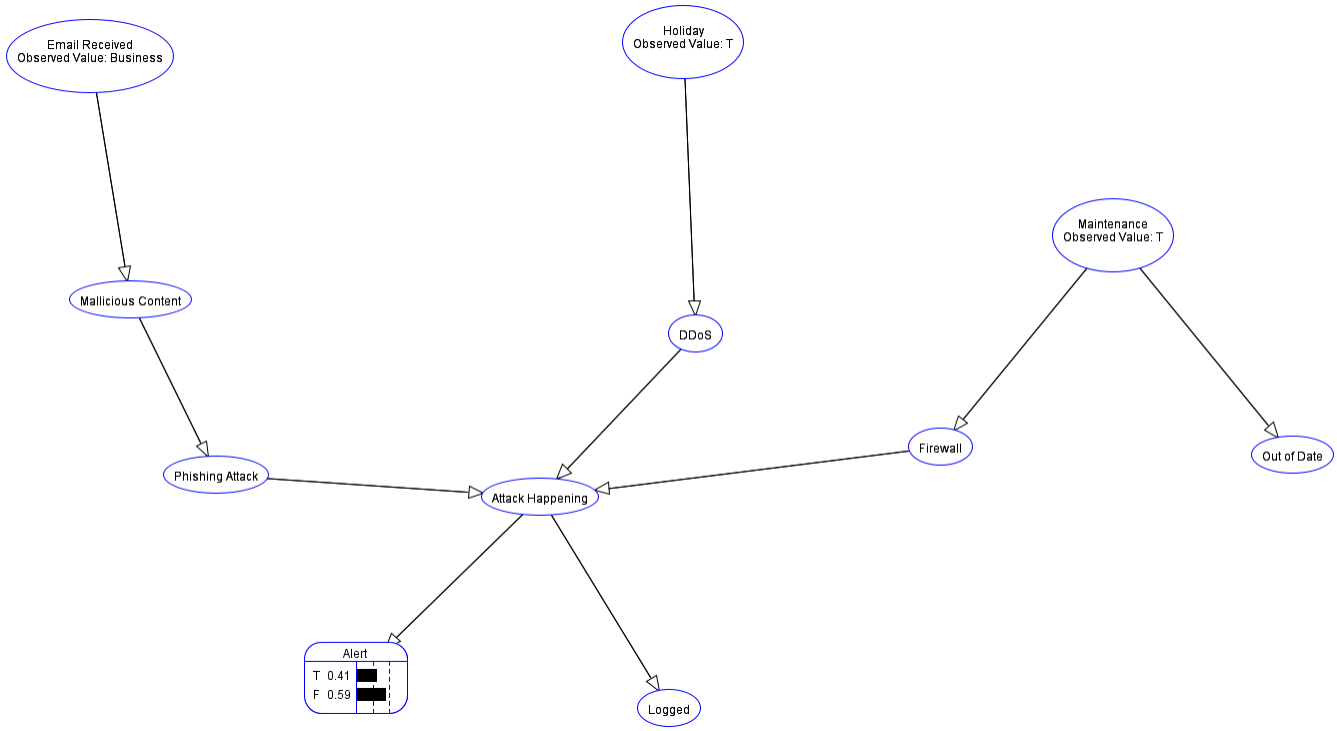

Figure 5: BN 1 Predictive query

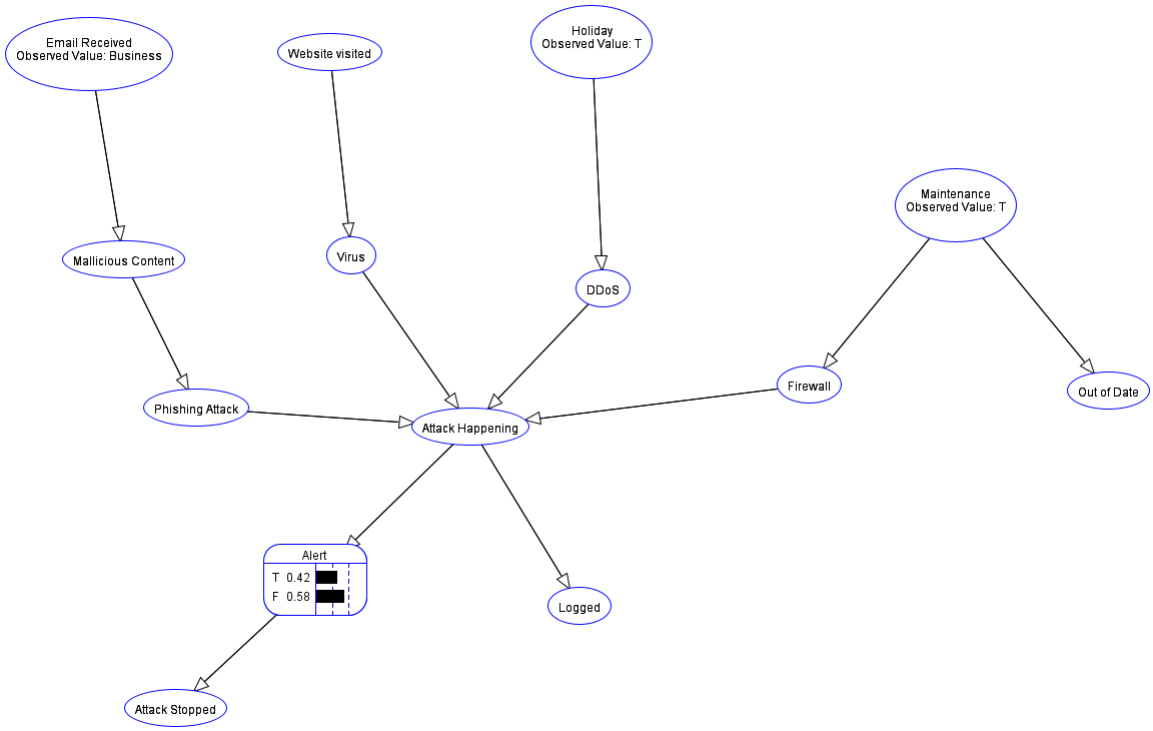

Figure 6: BN 2 Predictive query

Here it can be observed that in BN 1, there is a 41% chance an alert will be raised given the observed features. However, in BN 2, there is a 42% chance of an alert being raised. This is because of the extra attack.

1.3.3 Profiling

At any given point with no observations, the probability that an attack is happening within BN 1 is 25% and 27% in BN 2 (the extra attack raising the probability). By deactivating the firewall (observing it to be false) the chance of an attack rockets up to 44% and 46% respectively. If we observe that all possible attacks are true, but the firewall is unobserved, there is a 50% risk, whereas BN 2 has a 60% risk (again, the extra attack boosts the probability). By also observing the firewall is true, the risks do not change (since there was already a 95% chance of it being on anyway). However, by observing the firewall as false, both networks give a 95% risk of an attack. This clearly shows the behaviour of the firewall, and how without it, the system has a much greater risk of attack.

2 Literature Review

The paper in my references gives a detailed explanation of what Bayesian Networks are, and the proceeds to go through an example of how such a network can be used to diagnose patients based on their symptoms. This sort example was one that came straight to mind. Different combinations of symptoms can lead to different diagnoses. The paper also contains many references describing uses of Bayesian Networks within the medicinal world.

I think one of the most famous applications of Bayesian Networks was with IBM Watson. Originally, Watson was built to play Jeopardy, an American game show. However, he has now been re-purposed to aid medical

professionals in diagnosis. Using same machine learning techniques it harnessed to beat the worlds best Jeopardy players, it now has a higher correct diagnosis rate than most doctors.

3 Evaluation and Conclusion

This practical has been a great way to gain a practical understanding of how Bayesian Networks function, and how they can be a useful tool in working with conditional probabilities. I am confident in the design of my network, as it shows a clear logical connection between all elements, and the observed behaviour makes sense. I unfortunately didn't get to attempt part 2 due to time constraints regarding exams, but I am happy with my answers for Part 1.

4 References

http://www.cs.kun.nl/ peterl/eunite.pdf
https://www.top500.org/news/watson-proving-better-than-doctors-in-diagnosing-cancer/